NO SECRETS IN THE CHURCH: THE IMPLICATIONS OF THE DATA PROTECTION ACT 1998

JAMES BEHRENS
Chancellor of the Diocese of Leicester[1]

1. INTRODUCTION

The Data Protection Act 1998 came into force on 1 March 2000. It replaced the Data Protection Act 1984,[2] and implements the EU Data Protection Directive 95/46/EC. This paper examines its implications for the Church.

One of the key changes brought about by the 1998 Act is that the rules for data protection apply now to paper-based files as well as to computer files. So, for example, in general you must tell people that you have personal information about them, whether that information is kept on a computer or in a manual filing system. There are also some changes of terminology: *application for registration* is called '*notification*', *data user* now becomes '*data controller*', the *Data Protection Registrar* is now known as the '*Information Commissioner*';[3] the *Data Protection Tribunal* is now the '*Information Tribunal*',[4] and the *Data Protection Office* has been renamed the '*Office of the Information Commissioner*'.[5]

Incumbents and PCCs should identify a person responsible for compliance with the Act.[6] They need to consider whether to notify under the Act. They need to ensure that the church complies with the 'data protection principles'. They need to prepare for people making a 'subject access request'. At the diocesan level, bishops and others involved in diocesan administration need to reconsider the way they manage their private files. The same applies to the national Church institutions. In short, the Act affects the Church at the parish, the diocese and the national level.

[1] This paper is based on a lecture delivered on 7 November 2001 as one of the Ecclesiastical Law Society London Lectures.
[2] For the position under the Data Protection Act 1984, see James Behrens, 'Data Protection and the Church of England' (1996) 4 Ecc LJ 470, and James Behrens, *Practical Church Management* (Gracewing, 1998), chapter 12.
[3] Freedom of Information Act 2000, ss 18(1), 87(2)(a).
[4] Ibid, s 18(2); Freedom of Information Act 2000 (Commencement No 1 Order 2001, SI 2001/1637), art 2.
[5] Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; Tel: 01625 545700; Fax: 01625 524510; Web: www.dataprotection.gov.uk.
[6] See 'The Data Protection Act 1998, A Guide for Parishes' (London, Archbishops' Council of the Church of England, August 2001). This is available from Mrs Heather Roberts, Business Continuity Co-ordinator to the Archbishops' Council, Elizabeth House, 39 York Road, London SE1 7NQ; Tel: 020 7898 1178.

2. REGISTRATION

In general, any person or organisation which processes or handles personal information, i.e. information about identifiable living people, needs to be registered. The annual fee to maintain your registration is £35.

You do not need to be registered if you keep personal information only for your personal, family or household affairs, including recreational purposes.[7] If a local church member keeps personal information in connection with his church work—for example, the organist who keeps a record of the names, addresses and telephone numbers of members of the choir—the church member does not need to be registered, because it is the local church rather than the church member who is the 'data controller'.[8]

PCCs, incumbents and priests-in-charge who keep records just for staff administration, for dealing with accounts and records, and for general church administration no longer need to be registered. But if records are kept for pastoral care, then the person keeping the records needs to be registered. Most clergy are likely to keep notes or correspondence relating to such discussions, and should therefore be registered.

Others who need to be registered include diocesan bishops, suffragan bishops, diocesan chancellors,[9] diocesan registrars,[10] diocesan child protection officers, archdeacons, the diocesan board of finance,[11] the diocesan parsonages board,[12] deans and chapters of cathedrals, and theological colleges. Boards such as diocesan advisory committees do not need to be registered, because they lack legal personality, but the individuals who are members of the board may need to be.[13] At the national level, the Church Commissioners, the Central Board of Finance of the Church of England, the Church of England Pensions Board, the Archbishops' Council, and Lambeth Palace are all registered.

[7] Data Protection Act 1998, s 36.

[8] An employee is not a 'data processor' as defined in ibid, s 1(1).

[9] Even if the chancellor's filing system is entirely parish based, a filing system which allows the chancellor to look up the name and address of the vicar of a particular parish is within the definition of a 'relevant filing system' in ibid, s 1(1). If, as is likely, the chancellor keeps records of other names and addresses, then he should certainly be registered.

[10] The same point can be made about registrars. It is arguable that a registrar's activities are not sufficiently independent of the bishop and the diocese so as to make the registrar a data controller rather than a data processor. The safer course is to notify.

[11] The diocesan board of finance is a company, and so has legal personality: Diocesan Boards of Finance Measure 1925, s 1.

[12] The diocesan parsonages board is a 'body corporate', and so has legal personality: Repair of Benefice Buildings Measure 1972, s 1(5).

[13] See the definition of 'data controller' in the Data Protection Act 1998, s 1(1): 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.'

3. DATA PROTECTION PRINCIPLES

The data protection principles now apply to everyone who holds personal information, whether or not they are registered. So PCCs and others who may not need to notify must still ensure that they comply with the data protection principles.

In summary, the eight data protection principles are as follows:

1. You must use personal information fairly and lawfully.
2. You must only obtain and use personal information for the purposes you have specified in your registration. In general you must inform people what you are going to do with personal information about them, and give them the opportunity to opt out.
3. The information you hold should be adequate, relevant, and not excessive for the purposes you have it.
4. It should be accurate and, where necessary, kept up to date.
5. It should not be kept longer than necessary for the purpose for which you obtained it.
6. You must allow individuals their right of 'subject access'.
7. You must take suitable steps to keep the information secure against unauthorised or unlawful processing, and against loss or damage.
8. You must not allow information to be transferred to any country outside Europe which does not have adequate data protection.[14]

They will now be examined in more detail.

(1) *Fair and lawful use*

Churches should normally obtain a person's consent as to how information about them will be used.[15] So, for example, it is not fair use to include a person's address in a diocesan directory published on the internet without first obtaining that person's consent. (This example is also a breach of the eighth data protection principle, discussed below.) Parishes should therefore inform people before they publish their contact details, and offer them the opportunity to opt out.

Special rules apply to what the Act calls 'sensitive personal data'.[16] This will apply to much personal information held by churches. Anything to do with churchmanship or beliefs, and many matters concerning a subject's personal life, are likely to be 'sensitive'. Even a person's name and address becomes 'sensitive' if it is included on a church address list, because inclu-

[14] Data Protection Act 1998, s 4(1), Sch 1.
[15] Ibid. s 4(3), Sch 2, para 1.
[16] Ibid. s 2.

sion on such a list carries with it an inference of the person's religious beliefs. The first data protection principle has additional requirements where sensitive personal data is concerned,[17] but in the case of churches these requirements will be satisfied where the sensitive information relates only to members of the church, and the information is not disclosed to third parties without the person's consent.[18]

The difficulty comes when the church exercises its mission[19] to non-members.[20] In many cases priests are asked to provide pastoral support to relatives of someone who has died, where the relatives may well not be church members. The church cannot rely on the church-member exemption when it carries out its ministry to non-members. Here it is essential to obtain their 'explicit consent' to handling sensitive information.[21]

(2) *Use only for specified purposes*

If you are registered, you must only use personal information for the purposes listed in your registration. If you are not registered, which will apply to many churches, you must inform people of your reasons for keeping personal information about them, and what you are going to do with the information, and give them the opportunity to opt out. For example, a church should not make available a person's name and address to other organisations unless the church's registration mentions this as a purpose, or unless the church has notified the person that it may wish to do this. People have a right to prevent information about them being used for direct marketing.[22] In cases where disclosure is permitted, the church should ensure before disclosing the information that the recipient undertakes that the information will not be passed on further.

(3) *How much to keep*

Beyond saying that personal data is to be 'adequate', the 1998 Act does not oblige a church to keep any information which the church would rather not keep. If the church has material about a person which the person would be entitled to see,[23] and the church would be embarrassed if this material were disclosed, the church may decide to destroy the information. But a church

[17] Ibid, Sch 1, Pt I, para 1(b), Sch 3.
[18] Ibid, Sch 3, para 4.
[19] Parochial Church Council (Powers) Measure 1956, s 2; or, for a greater authority, Matt 28:19.
[20] Whether a person is a 'member' of the Church of England is not always straightforward: see James Behrens, *Confirmation, Sacrament of Grace* (Leominster, Gracewing, 1995), pp 78-79.
[21] Data Protection Act 1998, Sch 3, para 1. The expression 'explicit consent' is not defined in the Act. It is arguable that if the PCC holds data about non-members, this might be covered by Sch 3, para 7 (b), as it is an exercise of the functions of the PCC under the Parochial Church Council (Powers) Measure 1956, s 2. But by far the safest course is to obtain the 'explicit consent' of non-church members when making records of their personal information.
[22] Data Protection Act 1998, s 11.
[23] I.e. by making a subject access request under ibid, s 7.

cannot wait until it receives a subject access request and then destroy information so as to avoid disclosing it: any weeding out of files must be done before a subject access request is made.[24]

(4) *Accuracy*

It is not enough for a church to rely on information given by a third party. The church still has to take 'reasonable steps' to ensure the accuracy of the information. The reason why the information was obtained from the third party, and what the church intends to do with the information are both relevant in deciding what amounts to reasonable steps in any particular case.[25]

(5) *How long to keep information*

It is common for formal warnings to be removed from an employee's file after a year if there has been no further disciplinary action. Certain allegations about particular persons may need to be kept for much longer, perhaps indefinitely. Certain data may have an archival interest, and should be kept for this purpose. The subject of archives is discussed below.

(6) *Subject access*

The sixth data protection principle refers to the subject access rights, discussed below.

(7) *Security*

This covers security over both computer files and paper files. Churches need to have procedures setting controls over who can access certain files, whether the files are computer- or paper-based. Sensitive material needs to be locked in filing cabinets. Sensitive computer files may need to be password-protected, and there needs to be suitable measures to recover data in the case of loss. That does not mean that a church has to keep a copy of every paper file in a separate location: but it should certainly consider doing this for some files. Computer files are easily backed up, and this should be undertaken regularly.

(8) *The Internet*

Publishing information on the Internet is publishing it world-wide, which includes publishing or transferring it to countries which do not have a proper data protection policy. This is prohibited unless a person has given his consent to the transfer.[26] It is therefore essential to obtain each person's consent before publishing their personal information on the internet.

[24] Ibid. s 8(6).
[25] Ibid. Sch 1. Pt II, para 7.
[26] Ibid. s 4(3), Sch 4. para 1.

4. MANUAL RECORDS

The most significant change brought about by the Data Protection Act 1998 is that manual records, i.e. standard paper files, become subject to the data protection principles. Not all manual records are included—only those which form part of a 'relevant filing system'. That means structured in some way either by reference to individuals or in such a way that specific information relating to a particular person is readily accessible. Most plainly this would include a card index system. It probably also includes a correspondence folder kept in alphabetical order of surname.[27] Papers for PCC meetings and PCC minutes would not be a 'relevant filing system'.

As from 24 October 2001, you must inform people if you have any manual records about them, and why you are keeping these records.[28] These people have a right to make a subject access request covering these files. You must also take proper measures to protect the files from unauthorised access and from accidental loss. Any new manual records you create after 23 October 2001 will be subject to all eight data protection principles. In practice this means that unless your pre-October 2001 records are kept separate from your new records, you need to comply with all eight data protection principles for all your records. From 24 October 2007 all manual records whenever they were created will be subject to all eight data protection principles.

There is no subject access right for manual files which are retained simply for the purpose of historical research.[29] But this is a very limited exemption, discussed below, and would not apply to the usual case of files which are deposited with the diocesan archives.[30]

5. RIGHTS OF ACCESS

Unless an exception applies people have a right to be told if you hold personal information about them, why you are holding it, and what you are going to do with it. They also have a right to be told what the data says about them.[31] The 1998 Act uses the expression 'the subject access rights', which means the right to know what the data says. The Act also uses the expression 'the subject information provisions', which means disclosing both that you have records and what the records say.[32]

[27] It is arguable that such a file contains not specific information about a person but simply general correspondence with or about that person. As against this, a file of complaints about an incumbent kept by a bishop is there to give the bishop specific information about the complaints made about that incumbent. The file is therefore part of a 'relevant filing system', and is subject to the data protection principles.
[28] Data Protection Act 1998, s 39, Sch 8, para 14(2)(a).
[29] Ibid, s 33, Sch 8, Pt IV (paras 15–18).
[30] The exemption for historical and statistical research still continues after 24 October 2007: ibid, Sch 8 Pt IV.
[31] Ibid, Sch 1, Part II, paras 2 (1) and 3 deal with the *who* and *why*. Section 7 (of the Act itself, not the Schedule) deals with the *what*.
[32] Ibid, s 27(2).

To exercise their right a person makes a written request,[33] and must pay the prescribed fee.[34] The maximum fee which may be charged is £10.[35] The person must also provide (if required) evidence to confirm his or her identity, and sufficient information to enable you to locate the information which the person seeks.[36] The request must be complied with 'promptly', and in any event within forty days.[37]

If you do not comply with a subject access request, the person may appeal to the Information Commissioner,[38] who may take enforcement action requiring you to provide the information.[39]

(1) *What detail must be disclosed?*

There are two principles here. The first is that in responding to a subject access request, you do not normally need to name names.[40] The second is that in general you must provide all the information you have about the data subject, unless it would require disproportionate effort to do so.[41]

Thus a bishop is not required to disclose the source of any complaint unless the person making the complaint has given consent to this,[42] or unless 'it is reasonable in all the circumstances to comply with the request without the consent of the [person making the complaint]'.[43] If the person making the complaint had expressly refused consent for their name to be disclosed, or the complaint was made in confidence, it is likely to be reasonable for the bishop not to disclose the source of the complaint.[44]

Suppose a bishop has received a mass of correspondence making complaints about a parish priest, and then receives a subject access request by that priest, how should the bishop respond? He should not simply photocopy every letter having blocked off the name and address of the sender, and send a copy to the priest; for the priest may well be able to identify the senders of the letters by their handwriting, or there may be other identifying features within the text.[45] It would almost certainly be disproportionate for the bishop to

[33] Ibid, s 7(2)(a). No special form is required.
[34] Ibid, s 7(2)(b).
[35] Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000, SI 2000/191, reg 3. There is no reason not to charge the full £10. Special fees are prescribed for particular types of data, such as credit reference details, and health and education records. These are not material to this paper.
[36] Data Protection Act 1998, s 7(3). This is consistent with the need to ensure the information is not disclosed to the wrong person.
[37] Ibid, s 7(8), (10). The forty days only start to run from the date the subject provides the information under s 7(3): see s 7(8) and the definition of 'the relevant day' in s 7(10).
[38] Ibid, s 42(1).
[39] Ibid, s 40(1).
[40] Ibid, s 7(4).
[41] Ibid, s 8.
[42] Ibid, s 7(4)(a).
[43] Ibid, s 7(4)(b).
[44] Ibid, s 7(6)(a), (d).
[45] See the words 'who can be identified from that information' in ibid, s 7(4).

have to type up every hand-written letter before sending it to the priest, or to have to edit every letter in a whole pile of correspondence. Similarly, it would almost certainly be disproportionate to require the bishop to write to every complainant to seek their consent to disclosing their letter to the priest.

One practical solution would be for the bishop to précis the correspondence without naming names. He may, for example, state that between certain dates he received 35 confidential letters of complaint by parishioners relating to the incumbent's handling of the annual parochial church meeting. This may not be sufficient compliance for every case, but it should cover the majority.

(2) *References for ordination, employment and appointments*

A person does not have subject access rights in relation to references for education or employment, or for appointments to any office. He has the right to know that his employer has made a reference about him, but he has no right to see the reference itself.[46] This covers all church employments and appointments to any office, and in particular all church appointments made by the bishop or a patron.[47]

The official view of the Office of the Information Commissioner is that this exemption is only for references *given* by a data controller: no exemption is given for references *received* by the data controller.[48] Take the case where A writes to B with a reference about C. The exemption prevents C having subject access rights as against A, but the official view is that it does not stop C having subject access rights as against B.

The Office of the Information Commissioner considers this applies even if A does not want C to be able to see the reference by asking B to show it to him, and even if A makes this explicit by writing to B stating that he does not want the reference disclosed to C, or by endorsing this on the reference itself.

It may be possible to make A's reference anonymous (e.g. by only copying the text of the letter, removing the letter heading, and the name and reference of the writer), and if this is sufficient to prevent A being identified, then C will be entitled to see A's reference even if A does not consent. But in the case of many church appointments, this course would not succeed in preventing A being identified. In this case, and if A refused consent, C would then only be entitled to see the reference 'if it is reasonable in all the circumstances to comply with the request without the consent of the other individual'.[49] From the point of view of all three parties the result is highly

[46] Ibid, s 37, Sch 7, para 1.
[47] Thus, for example, the appointment of a new assistant curate is an appointment to an office. Assistant curates are not employees: *Coker v Diocese of Southwark* [1998] ICR 140, (1998) 5 Ecc LJ 68, CA.
[48] *The Data Protection Act 1998, An Introduction* (Office of the Information Commissioner, 1998), section 3.1.
[49] Data Protection Act 1998, s 7(4)(b). Section 7(6) sets out considerations to help decide whether it is reasonable in a particular case to disclose the contents of the reference.

unsatisfactory. A can never be certain that his or her reference about C will not be disclosed to C even if he specifically refuses consent; it is not clear to B whether he is under a duty to disclose A's reference to C; and it is not clear to C whether he is entitled to see A's reference about him.[50]

A robust challenge to this official view is called for. Surely if a reference is given in confidence, it must be received in confidence. If the confidentiality of written references can no longer be relied upon, the result will be an increase in the number of references which are given only orally, so that there is no written record of what is said. This will lead to increased secrecy, the very evil which the 1998 Act and the EU Data Protection Directive 95/46 EC sought to attack.

A strict literal construction of the provision seen in isolation does support the official view. But when the provision is seen in the context of other exemptions in Schedule 7 of the Act, there is much to support the argument that the exemption must be given a purposive rather than a literal construction.[51] A purposive construction would be to say that the words 'given by the data controller' does not prevent references remaining confidential once they are received. There is nothing in the EU Data Protection Directive which prevents this purposive construction.[52] Nor is there as yet any decision on the point.

If the Church wishes to maintain confidentiality over references, it needs to challenge the official view. One possibility is to wait for the Office of the Information Commissioner to take enforcement proceedings against a person refusing to disclose a reference in a particular case, and this can become a test case for resolution by the High Court.[53] The Dean of the Arches has suggested a better course, namely drawing the point to the attention of the Office of the Information Commissioner, so that further guidance notes can

[50] *Data Protection Act 1998 Subject Access Rights and Third Party Information* (The Office of the Information Commissioner, 2000) highlights the difficulties faced by a person who has received a subject access request where the third party has refused consent for disclosure. The guide is available on the Office of the Information Commissioner's web site http://www.dataprotection.gov.uk/.

[51] Compare, for example, the exemption for personal data processed for the purpose of judicial appointments and honours (Data Protection Act 1998, Sch 7, para 3), and personal data processed for the purpose of Crown or Ministerial appointments (Sch 7 para 4, as implemented by the Data Protection (Crown Appointments) Order 2000, SI 2000/416). In both these cases, data is exempt both when it is given and when it is received. There is no logical reason why references for these public appointments should be treated differently from references for ordinary employments and appointments.

[52] It is noteworthy that the Explanatory Note to the Data Protection (Crown Appointments) Order 2000, SI 2000/416, states that the Order 'contributes to the implementation of' the Directive, even though the effect of the Order is to remove the right of subject access in the case of the crown appointments listed in the Order.

[53] Enforcement notices are made under the Data Protection Act 1998, s 40. There is a right of appeal from an enforcement notice to the Information Tribunal under s 48, and a further appeal from the Information Tribunal to the High Court on a point of law under s 49(6).

be issued on the subject. This has now been done,[54] but the Office of the Information Commissioner has not changed its official view. As a last resort the Church may wish to make representations in Parliament and press for a suitable amendment to the legislation.[55]

(3) *Senior church appointments*

The Data Protection Act 1998 allows records relating to possible senior appointments within the Church of England to be kept.[56] But this is a separate issue from keeping such records confidential from the subject of the records, i.e. preventing a member of the clergy from knowing what is said about him in these records.

The Data Protection (Crown Appointments) Order 2000 grants exemption from the subject information provisions of the Act[57] to personal data processed for the purposes of assessing any person's suitability for any of the following Crown appointments:

- Archbishops, diocesan and suffragan bishops in the Church of England;
- Deans of cathedrals of the Church of England;
- Deans and Canons of the two Royal Peculiars;[58]
- The First and Second Church Estates Commissioners.[59]

The current practice is that the Archbishops' Secretary for Appointments contacts all the diocesan bishops every year to ask if there are any clergy within the bishop's diocese who should be considered for senior appointment. Whilst the position about confidentiality of ordinary employment references is far from clear, persons hoping for one of these Crown appointments have no right to know whether anything has been said about them to the Archbishops' Secretary for Appointments.

[54] Sheila Cameron QC, 'Data Protection Act 1998 Confidential References' (24 July 2001, unpublished).

[55] In the House of Lords, the government was asked to introduce an amendment to the legislation to include confidential references *received* by the data controller. The government minister, Lord Falconer, replied stating 'we believe that normally, unless there is a special situation, that [section 7(4)] would mean that references from another person to the data controller would not have to be disclosed, which would seem adequate protection under the circumstances'. Section 7(4) is the section stating that sources of information do not normally have to be disclosed. I am grateful to Anna James of Lee Bolton & Lee for drawing my attention to this.

[56] Data Protection Act 1998, Sch 2, para 5 (c), (d).

[57] I.e. both the right to know whether there is any information about you, and the right to know what it says about you.

[58] This presumably refers to Westminster Abbey and St George's Chapel, Windsor, and not to the three Chapels Royal (St James' Palace, St Peter ad Vincula in the Tower of London, and Hampton Court Palace). The three Chapels Royal have a Dean and a Sub-Dean, but no Canons: see the *Report of the Review Group on the Royal Peculiars* (London, Church House Publishing, 2001), chapter 6. The report is also available at www.open.gov.uk/lcd/majrep/royalp.htm.

[59] Some non-ecclesiastical Crown appointments are also mentioned in the Data Protection (Crown Appointments) Order 2000, SI 2000/416.

(4) *The 'Caution List' and clergy discipline*

When the Caution List is put on a statutory footing in the new Clergy Discipline Measure,[60] it will obtain a blanket exemption from the subject information provisions.[61] Until this happens, files kept for the purpose of clergy discipline concerning dishonesty, seriously improper conduct, unfitness or incompetence on the part of the clergy, will in most cases be covered by an exemption for those involved in regulatory activity.[62]

As in the case of a criminal investigation, a file is built up before a decision is taken whether there is sufficient evidence to bring a charge. The regulatory exemption should cover the preliminary stages of the disciplinary process, as well as the proceedings themselves. It may also cover 'peripheral' stages. The question in each case is whether the subject access rights would 'be likely to prejudice the proper discharge of the [disciplinary process]'.

The Information Commissioner takes the view that 'likely to prejudice' in section 31(1) means that there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged.[63] The Information Commissioner is probably right in saying that the circumstances of each case must be looked at individually, rather than treating the matter as a blanket exemption, but the requirement should be easily satisfied in the case of most church investigations. It would normally be highly prejudicial to the investigation if the file was not confidential from the very beginning.

6. BISHOPS' PRIVATE FILES

The first point about bishops' private files is that they are almost certainly manual records. The second is that if the bishop is any good at administration at all, these files are probably sufficiently structured to be within the Data Protection Act 1998 .

Applying the data protection principles, bishops must now:

- inform their clergy that they hold records about them;
- permit the right of subject access, except where an exemption applies;
- keep files secure and confidential;
- not keep files longer than necessary.

This applies both to existing files and to any new files created after 24 October 2001.

[60] Clause 35 of the draft Clergy Discipline Measure imposes a duty on the archbishops acting jointly to compile and maintain what is now known as the 'Caution List'.
[61] Data Protection Act 1998, s 31(2)(a)(iii), (3)(a).
[62] Ibid, s 31(3)(c).
[63] *The Data Protection Act 1998, An Introduction* (Office of the Information Commissioner, 1998), sections 2.4 and 2.2.4.

(1) *Informing clergy*

Bishops must inform their clergy that they hold records about them, and why. This can be in the form of a standard letter, without descending into particulars of exactly what information the bishop has about each particular incumbent.

(2) *Subject access*

Bishops must permit the right of subject access, except where an exemption applies. So anyone can require the bishop (on payment of the statutory fee) to supply a copy of the information the bishop has about them, unless an exemption applies. Most of the difficult cases will concern the bishop's correspondence files concerning problem clergy, discussed above under the heading 'What detail must be disclosed?'.

(3) *Security*

Bishops will have to take proper steps to make sure that files are kept confidential from unauthorised access and loss. What this means in practice may need to be discussed centrally between the Church of England and the Office of the Information Commissioner.

(4) *Old files*

From a data protection aspect, bishops can, if they choose to do so, destroy their files instead of handing them on to their successor. The fifth data protection principle is that personal data shall not be kept for longer than is necessary for the purposes for which the bishop is registered to hold the data. In other words, there is a presumption that it is permissible to get rid of data when it is no longer needed. If a bishop considers the files should be destroyed when he retires, there is nothing in the Act to stop him.

In many cases bishops will want to keep files in the diocesan archives. Files that are deposited with the archivist 'for research purposes' may be kept indefinitely.[64] 'Research purposes' includes statistical or historical purposes, but only if the files are not to be used in order to take decisions concerning particular persons, or in such a way as to cause substantial damage or substantial distress to any person referred to in the files.[65] So a file which contained details of a disciplinary process against clergyman X in the year 1980 is not stored for research purposes if the bishop contemplates that he may need to look at the file in the future when dealing with clergyman X.

If files are deposited in the diocesan archives which are not just for research purposes, then anyone has a right to make a subject access request, and find out what information about them is contained in the files. If files *are* deposited only for research purposes, then there is no subject access right.[66]

[64] Data Protection Act 1998, s 33(3).
[65] Ibid, s 33(1).
[66] Ibid, s 33(4). Processing for research purposes requires that the results of the research or any resulting statistics are not made available in a form which identifies people mentioned in the files.

But I doubt this will be an effective means of ensuring confidentiality. If clergyman X wishes to find out what information is held about him relating to the disciplinary incident in 1980, there is nothing to stop him dressing up a subject access request in the form of historical research, and thereby seeing the file. He may, for example, say he wishes to investigate all cases of disciplinary process in the diocese of Y over the period 1975 to 1985.[67]

What then should be done by the bishop who has sensitive files, in order to balance the need to preserve confidentiality with the desire to preserve information for posterity? One possibility would be to sift through files before releasing them to the archivist. Those which do not contain sensitive information can be released without more ado. Those which do should have stamped on them words such as 'for diocesan archive, for historical or statistical research purposes only. Not to be disclosed without reference to me or my successor as bishop of Y.' The bishop may have no redress if the archivist ignores this instruction, but it may serve to preserve confidentiality in many cases where it does matter. It may be sensible for the bishop to issue some standing instruction to the diocesan archivist as to how to deal with these sensitive files, and how to handle any requests to see their contents.

7. AN APPRAISAL

What should our attitude be to all this? It is a welcome relief that PCCs and some incumbents no longer need to be registered. In contrast, from an institutional point of view it is an administrative burden that manual files are now subject to the Act. But from the point of view of the people referred to in these files, the Act is an expression of the openness and integrity which should be a part of the Church as much as a part of every Christian.[68]

Does the Act go too far in protecting the rights of people against the interests of those who hold personal information about them? All PCCs and vicars are now obliged to inform their parishioners if they hold records about them, and the purposes for which these records are held. In practice this means that when people join the church they should be told that the details they give the church will be entered onto the church filing system—something they would no doubt assume would take place anyway. This is unlikely to cause any difficulty in normal cases dealing with church members. Before keeping sensitive information relating to non-church members, the church must obtain their 'explicit consent'.

It is when one moves beyond the parish to the diocesan level that the Act presents most difficulties. Information given in confidence should be received in confidence.[69] If a recipient of a reference given in confidence is obliged to disclose it to the employee, the Act places the interest of the employee before

[67] The Data Protection Act 1998 recognises that files may be disclosed to a person who is mentioned in the files, in the context of research: s 33(5)(b), Sch 8, para 18(b).
[68] See e.g. Eph 4 : 17–32.
[69] Prov 11 : 13.

the interest of the Church. This may lead to a worse culture of secrecy than the Act sought to remedy. If references intended to be confidential are now not so, the balance between the individual and the institution is wrong. The Church should challenge this interpretation.[70]

The Act presents a threat to the preservation of the tradition of the Church. Today's files become tomorrow's history. The protection and confidentiality given to materials stored for archive purposes is insufficient to prevent a determined, and perhaps unscrupulous, person seeking to obtain access to the information in sensitive files for purposes other than genuine research. Some files which prior to the Act would have been preserved for history will no doubt now be destroyed, to prevent their contents becoming known to people mentioned in them. Despite recognising the need for the preservation of history, the Act fails to deal adequately with the problems this raises.

In 2001, when the right of subject access to manual files was about to become law, there were some gloomy predictions that there would be a flood of subject access requests. These predictions have proved unfounded. One year on I am aware of a few subject access requests which have been made, but the numbers involved are very small. So far as Leicester is concerned, neither the bishop nor the diocesan secretary has had any requests at all. It is business as normal.

[70] The problem about employee references is not limited to clergy appointments. It affects all parish lay employments as well. But I see its *institutional* danger at the diocesan level.