

GDPR Parish Q&As

	Topic	Question	Answer
1.	1.1 Baptism / marriage records	1. Q: What about people asking for baptism or marriage records?	A: If the request is for someone else's data then ask if that person knows that the data is being requested? The GDPR only applies to living individuals.
2.	2.1 Births, deaths & marriages	2. Q: The parish magazine includes extracts and photographs from the registers of births, marriages and funerals; do I need consent to share this data?	A: Not funerals because GDPR only affects living people. You do need it for births and marriages. You might want to get this during the application process.
3.	3.1 Births, deaths and marriages	3. Q: What about historic information kept on websites: e.g. births, death, marriages, etc in newsletters.	A: How likely are the data subjects to complain? When privacy notices are renewed some people may come forward and ask to be removed from mailing lists. You should react appropriately by removing their data
4.	4.1 CCTV	4. Q: Are there any GDPR requirements about CCTV?	A: The law covering CCTV isn't changing; but the sanctions are becoming tougher. You need to display a sign letting people know that CCTV is operating. This must name the data controller and give their contact number. There is also an ICO code of conduct available on the ICO website. If the CCTV covers public areas then you may require a SIA licence. The entrance to church and the car park is private but the street is public. There are also rules about the size of lettering which must be used. You might use a generic email address such as "dpo@...".
	4.2 CCTV	5. Q: Is CCTV subject to GDPR?	A: Yes. Film and photos are personal data. If you have CCTV which is managed by a third party then they only need to abide by GDPR if they can see the data. If they cannot see the data then GDPR does not apply to them. You must put a sign up notifying people of their rights.
	4.3 CCTV	6. Q: CCTV – a church has it and what about the recording of individuals?	A: Images are personal data. If installed after 25th May a Data Protection Impact Assessment may be needed. You must also have the correct signage in place including details of the Data Controller and/or the Data Protection Officer. If the CCTV covers public spaces (e.g. the pavement or road outside the church) then you may require a licence to install CCTV.
5.	5.1 Charity Commission	7. Q: How is GDPR applicable to the returns which are made to the Charity Commission	A: It is best to be really transparent by saying "these are the parties we share information with and this is why ..." The sample privacy notice in the GDPR Toolkit tries to list all the relevant ones but if something has been omitted please let us know.

	Topic	Question	Answer
6.	6.1 Children	8. Q: Is it correct that children of 13 and over can give consent when the Children's Act says children are children until the age of 18	A: We are not changing the definition of a child merely that the age of consent for data protection purposes which is 13 from 25th May.
7.	7.1 Compliance	9. Q: Implementation and responsibility – where does responsibility end? E.g. what happens if the vicar and others in the parish aren't really bothered.	A: The legal responsibility rests with the PCC rather than individual officers or with the vicar in respect of pastoral information obtain by them in their official role
	7.2 Compliance	10. Q: What happens if you haven't got all the consents in place by 25th May 2018?	A: Be realistic and practical. Have a plan to be compliant.
8.	8.1 Consent	11. Q: How do you record oral consents?	A: One example might be to use an Excel spreadsheet. This might be the same place as you record how people want to be contacted. Tip: Younger people are typically happy to use more intrusive methods of communication. If you do not specify how you will communicate (e.g. phone, email, post) then you will have fewer responses.
	8.2 Consent	12. Q: In the past people completed cards to say that that wanted to receive the newsletter. The paper copy was shredded so we don't have actual proof that consent was given. Do we need to get a new consent?	A: The law on consent law is changing – one of the new things for which consent is required is marketing i.e. anything which furthers the activities of the church. The ICO considers newsletters to be marketing. Therefore you would need to look at what the existing consent covers. Importantly, to be valid in the future it must be opt-in . If consent was obtained in that way it is GDPR compliant. If it was obtained using "opt-out" then you would need to obtain a new consent. Consent doesn't have to be in writing but can be obtained verbally. For example: at a meeting the email addresses of all attendees might be collected and the chair may ask if attendees would be ok to receive information in the future using those email addresses. If anyone does not agree to receive newsletter their details would need to be removed from the list of email addresses collected. It is a good idea to keep a record of how the consent is obtained. The example consent form in the GDPR Toolkit gives a variety of options, plus space to add additional examples of the purposes the data will be processed for. So, even if the original consent form has been destroyed, having a list of those who have consented would be ok. It is a good idea to keep available an example of the consent although this is not essential. Some people may complain about receiving the newsletter but this is easily resolved by taking them off the list of recipients. People generally complain about data privacy if they have another axe to grind.
	8.3 Consent	13. Q: A segmented consent is difficult to administer can't we just have a single consent?	A: The consent form in the Toolkit has been designed to broadly cover as wide a range as possible of the church activities. The key principle is to be transparent. You should not use personal data for a new purpose without

	Topic	Question	Answer
			informing data subjects beforehand. The new law gives control back to individuals and does not take into consideration that most people in churches may not worry about how their data is processed.
	8.4 Consent	14. Q: What is the shelf-life of consent?	A: Currently consent from a third party only lasts for 6 months. Guidance from the ICO suggests that consents should be updated every two years if being received from the person themselves. It is good practice to remind people regularly that they can withdraw their consent at any time, which must be as easy to withdraw as to give.
	8.5 Consent	15. Q: Rev Bloggs has told Mrs Church Warden that under GDPR she can't put people's name and address on the raffle stubs.	A: If they can't do that then how would you know that you have won? The key thing is the use of the data. If the tickets might be sold outside the church, you should not use the address details to email people again about a similar event in the future without asking for their consent. As another example if you have a business card for those who supply a service they aren't going to complain about you keeping their data although they will complain about not being paid on time.
	8.6 Consent	16. Q: For Consent – does the form have to list all existing activities or just those which start after GDPR comes into effect?	A: The draft Consent form in the GDPR Toolkit has tried to be all encompassing with different layers for you can receive information, you can get involved, and then anything else. This is using broad language. Do please contact the Diocese if you can think of a regular activity we have not covered. Consent should be specific – i.e. informed consent meaning that the person knows what they are agreeing to. The ICO regard consent as time-limited which will need to be renewed – you might do this at the same time as renewing the Electoral Roll.
	8.7 Consent	17. Q: If you have a new project do you need to ask for a new consent form to be signed?	A: Consent must be specific but can cover multiple projects. E.g. tick if you are happy to hear from us about activities in the parish.
	8.8 Consent	18. Q: How can we alert PCC Officers that we don't need to seek their consent?	A: The privacy notice does this.
	8.9 Consent	19. Q: How long do records of consent need to be kept?	A: As you are required to regularly refresh consents, you should keep the records until the next time you refresh consent.
	8.10 Consent	20. Q: Can information of visitors who attended services be used, for example, to create a mailing list for future events?	A: No! Not unless they had completed a consent form.
	8.11 Consent	21. Q: Do I need to spell out how I will communicate? E.g. by mail, by phone etc.	A: Yes, you should. The ICO recommends that consent forms use a variety of ways in which to approach different audiences, e.g. social media. A variety of approaches usually leads to a better response rate.

	Topic	Question	Answer
	8.12 Consent	22. Q: What is the best type of consent language to use?	A: See the consent form in the Toolkit appendices. The word “consent” is more formal but it is clearer than the word “agree”
	8.13 Consent	23. Q: Rotas – have e mail distribution list etc.	A: You can get consent orally and point them to the privacy notice and make a note you have done this.
	8.14 Consent	24. Q: Person running programme of concerts and films has a mailing list from those who attended previous events.	A: At the next event ask them to reconfirm their e mail address and add consent details
	8.15 Consent	25. Q: Consent forms and getting them retrospectively – does previous verbal consent count?	A: Verbal consent is OK but it will need to be recorded. After 25th May consent changes (e.g. previously it was generally an “opt out” approach and now it is an “opt in” one) and generally by implication but after 25th May it will need to be more explicit so you will need to be more specific going forward
	8.16 Consent	26. Q: If you are saying we can’t use consent forms for volunteers then lots of people will be covered as they are volunteers in some capacity so would it be better just to rely on other legal reasons and not worry about consent?	A: In employment and volunteer roles consent doesn’t work as there is a need to process their data for their role to function. However if you are using their data for a purpose unconnected to their role (e.g. sending a fundraising letter) then you would need to get consent.
	8.17 Consent	27. Q: If I send consent forms to everyone on our electoral roll and lists they sign and give them back is that job done and is an electronic response OK?	A: Electronic, verbal and written responses are all OK but there must be a record kept of responses and people must be pointed to the privacy notice. Going forward you need to have a process in place for new people.
	8.18 Consent	28. Q: If we have a clear photo of children on our database but don’t have specific consent do we need to get consent?	A: The first question is do you need to have the photo? If so then yes you will need consent.
	8.19 Consent	29. Q: On the consent form there is a reference to receiving communication by social media but surely people already have to agree to do this by signing up etc? And would this cover use like WhatsApp?	A: You may want specific consent for WhatsApp as people can see the phone numbers for everyone in the group but generally at the moment the user themselves takes steps to opt in to its use. This is really about future proofing the form but for WhatsApp you will need specific consent.
	8.20 Consent	30. Q: WhatsApp involves sharing personal details – does this require consent?	A: People would need to give consent for this and also for adding a new person to the group. Verbal consent from the person whose details are being shared could be obtained but there would need to be a record. Personal details (and indeed other details) shared through social media exist in perpetuity – this needs to be explained clearly to the person concerned and how the social media platform will work. You can’t rely on a general consent as there is a need to be explicit about the details (e.g. that it will exist in perpetuity)

	Topic	Question	Answer
	8.21 Consent	31. Q: Do we need to get written consent when taking photos for the church from all people or just children? In the past we have used an "opt out" withholding of consent for photos, is that no longer allowed?	A: Yes, you should ask people for consent if you are going to use their photographs, particularly if they are going to feature on your website or newsletters. You will need parental consents for children under 13.
	8.22 Consent	32. Q: Is consent required to hold information on (say) Google contacts? Assuming these do not fall into the category of data processors as they are simply providing a platform to store/record data. Same points, on storing bank details on-line with bank for BACS/electronic payments.	A: If you are going to use your contacts for church purposes, e.g., add their names to a newsletter mailing list, then you should ask for consent.
	8.23 Consent	33. Q: The toolkit says lists of members do not require specific consent for churches (p5). Does this cover church members/attenders not enrolled on the Electoral Roll? Does this mean simple lists of names, or if we add information like contact details or other notes does consent become required?	A: Parishioners do not need to give explicit consent just to have their names on your mailing list unless you are carrying out marketing. There is an exemption for maintaining membership lists which also applies to religious organisations but you cannot share their data with third parties or use it for marketing without consent. The exemption is meant to cover administering a membership list and not all the purposes you might use data for.
	8.24 Consent	34. Q: My church has historically produced a paper address book annually which is distributed to all those included in it, so that church members can have each others' contact details. We have recently signed up to ChurchSuite which will mean we no longer need to have a paper address book (except for those with no computer access). I will obviously ensure I have everyone's permission (via consent form) to share their details with the rest of the church before launching ChurchSuite outside the staff team. My question is this: we do not have a record of who was given paper address books in the past. How do we manage/control data that has been distributed before GDPR was on our minds? Are we required to ask all church members to destroy or return old address books? If yes, we have no way of monitoring whether or not this actually happens. Please can you advise me?	A: You do not need to go back and fix your historical records for the old paper copies or ask for people to destroy them. The GDPR does not apply retrospectively but from 25th May onwards.
	8.25 Consent	35. Q: On the DoL template Consent Form... Yes, please I would like to receive communications by email does this opt-in mean we can contact an	A: Yes.

	Topic	Question	Answer
		individual by email using Mailchimp?	
	8.26 Consent	<p>36. As I drew up the agenda for a forthcoming PCC meeting a further query occurred to me:-</p> <p>I understand on the one hand that one needs consent to name someone when praying for the sick during intercessions (and presumably additional consent if one is to identify their sickness publicly) and, given that some sicknesses will mean the person lacks capacity to give consent, this would have to be asked for in advance on the consent form that non-role-holders tick and sign. Logically I would have thought this was a matter on which everyone could choose to give or withhold consent. Yet I understand that role holders should definitely not be invited to give consent for anything. Please clarify.</p>	<p>Role holders should not be asked for consent for processing their data in connection with their role.</p> <p>However role holders may have a dual role. They may also be donors who give gift aid. It would be appropriate to give them both notices and to ask for their consent for non-role holders matters such as donating etc.</p>
	8.27 Consent	<p>37. A consent question regarding Eventbrite.</p> <p>We have an annual event called Summer Lectures. We have an Eventbrite List of attendees which is used for this repeat event. Can I consider that my List of attendees have given opt-in consent to be invited to this years Summer Lectures because they provided their contact data when purchasing their ticket(s) to last years same event?</p> <p>Please could you advise - I understand that the list of attendees could not be used for anything other than the purpose of Summer Lectures. (I'm aware that: Eventbrite states that it is GDPR compliant; an attendee can unsubscribe on Eventbrite).</p>	<p>If their opt-in consent was GDPR compliant, i.e. it was expressed, unambiguous and freely given, then you do not need to ask for it again.</p>
9.	9.1 Contracts	38. Q: What about contracts with third parties?	<p>A: The PCCs should satisfy themselves that contractors and agencies that they use are GDPR compliant. Their approach to this task should be risk based e.g. check that payroll agency is compliant before checking that plumbing contractor is compliant. Contracts should name the relevant Data Controller.</p>
10.	10.1 Data Controllers	39. Q: Our parish has a branch of the Mothers Union whose finances are independent of those of the	<p>A: The Mother's Union is separate legal entity and a separate data controller. If the PCC and</p>

	Topic	Question	Answer
		PCC. This branch organises and runs a weekly community choir for people from the surrounding area. All monies raised from the choir and operating costs are taken into the branch's own accounts. The member of the Mothers Union branch who organises the community choir holds contact information for both members of the branch and the people who attend the choir. She believes that as the branch is part of the Mothers Union which is separately registered as a charity, the branch is therefore not a function of the parish and consequently it is the Mothers Union and not the parish which will be responsible for compliance to GDPR for that information. Is this correct?	the Mother's Union are carrying out any joint activities, you may be joint data controllers.
	10.2 Data controllers	40. Q: What is the difference between information held by the vicar and by the PCC?	A: Pastoral information (e.g. about relationships) is held by the vicar acting as data controller (would be the same in respect of info on bereaved families). The vicar is acting in their "official" capacity.
11.	11.1 Data Protection Officers	41. Q: Do we have to appoint a Data Protection Officer (DPO)?	A: The legislation has evolved through its drafting - and it now simply says that one is required if the entity is processing data on a "large scale". However, it is unlikely that the parishes in the Carlisle Diocese operate large scale personal data processing.
12.	12.1 Data retention	42. Q: How long should data be retained?	A: Subjects e.g. wedding couples should know / be informed about how long the info they provide will be kept. Employees; not all info will need to be kept e.g. information on hygiene concerns need not be kept but information on pensions would be.
	12.2 Data retention	43. Q: Past information and deletion – are there any guidelines about how long information should be retained?	A: With role holders there is a "natural" period of the time they are in the role and a "run off" period afterwards. There are other legal reasons to keeping information for a specific period. There are also certain items which need to be archived – you will need to consider on a case by case basis for each type of data
	12.3 Data retention	44. Q: Our church is wondering how long we should keep the details of our ex-members or for members who are no longer attending our church but haven't notified the church why they have left. Is there any legal reason we should still keep them for record purposes and if we cannot contact them to remove them from our database,	You can delete their records without asking for consent. You can decide how long to keep their data for before you delete it.

	Topic	Question	Answer
		can we delete their records after a certain time frame?	
13.	13.1 Data security	45. Q: Is having a password (e.g. on dropbox or Church Suite) sufficient security?	A: Having a password is the current minimum for security and highly sensitive data may need to be encrypted. What is good practice will probably change going forward.
	13.2 Data Security	46. Q: I've noted that Mailchimp should not to be used for sending confidential information. Is it ok to process peoples email addresses into the Mailchimp service?	A: Mailchimp states this in its terms because (a) Mailchimp does not want to be liable and (b) Mailchimp is not secure. You need to use other methods of security in addition to Mailchimp such as encryption, password protection, restricted access etc.
14.	14.1 Data sharing	47. Q: The different Dioceses, the church, and Bishops & other church institutions keep a lot of data. Is this appropriate?	A: The Diocese of Carlisle is working hard to ensure that it complies with GDPR and the National Church is also producing guidelines for the House of Bishops. Clergy have had the right to make a Subject Access Request on their "Blue File" since 2001.
15.	15.1 Data Subject access	48. Q: The vicar has various bits of data e.g. a copy of passports for a wedding couple. This would need to be disclosed if there was an SAR but what about all the e mail exchanges?	A: Only e mails that contain personal data would need to be disclosed (you would have to check each e mail). Personal opinions are personal data – i.e. you would need to sift through anything that mentions the person and check the content. There is also the issue of how long you need to retain data – so you would only need to keep copies of the passports until the marriage had taken place. All data like this needs to be password protected.
	15.2 Data subject access	49. Q: With data disclosure, are there limits accordingly to practicality? Searching emails for the text of a person's name is practical though searching through years of emails in case a name or a person's details are included in a non-searchable PDF or picture format file would be impractical.	A: You need to go to reasonable efforts to find data that is relevant to a person's data subject access request. There are software tools available that make searching for data easier. You are allowed to ask the requester to narrow the scope of their request but they have no obligation to agree to do this. They are entitled to their data (but not the documents)
16.	16.1 Deletion	50. Q: With deletion of data, how can an organisation ensure data held by a third-party is also deleted, if that third party is a former member/officer of the church, who no longer attends or has dealings with the church, and have no knowledge if personal information is retained on a personal computer from the time of their former connection? Is a request to that person to check and delete sufficient?	A: You should ensure the third party has a contractual obligation to comply and assist you to respond to requests. This is one of the contract clauses you are required to include.
	16.2 Deletion	51. Q: I assume deletion of data does not extend to archived printed/published records, such as church magazines from previous years that may contain contact information etc.	A: If you cannot easily extract the information to be deleted then you can retain it, particularly if you have a legal reason to keep it. You should keep a record of someone' request to have their data deleted particularly if you have not been able to fully comply.

	Topic	Question	Answer
17.	17.1 Electoral Roll	52. Q: What about Electoral Roll data?	A: It is a legal requirement to establish an Electoral Roll so consent for this is not required. The Electoral Roll falls under the exemption for religious organisations to keep a list of members. However, the information can only be used for membership purposes, and not for other purposes and certainly not marketing. If you want to extend the use(s) then you would need to obtain consent from those on the list to use their data for another purpose.
	17.2 Electoral Roll	53. Q: PCCs are legally obliged to maintain the Electoral Roll and this must be displayed in the church. Can someone withdraw their consent and if they can what happens?	A: The key thing here is that the Electoral Roll is not invalid if a person's address is not displayed. Therefore, you might have two different versions – the full Roll and the abridged version for display which includes names only. The roll is kept for legal reasons so consent is not relevant.
	17.3 Electoral Roll	54. Q: Our Electoral Roll form has a questionnaire on the back asking if the person would be willing to support the church in voluntary ways, for example through volunteering or financially. Is this considered to be marketing?	A: Yes. This is marketing so you need to obtain consent to process their data in other ways than just for the Electoral Roll.
	17.4 Electoral Roll	55. Q: How does the data collected for the Electoral Roll fit with GDPR?	A: Remember that the electoral roll is required under ecclesiastical legislation. GDPR simply requires that we are clearer with people about why we are collecting data. So, if we use the Electoral Roll data for other purposes we need to be transparent about all of the purposes that we are going to use the data for. This is achieved through the privacy notice.
	17.5 Electoral Roll	56. Q: We are required not only to compile the Electoral Roll but also to display it, often in a church which is open to the public. This seems to be a significant data breach. How can we resolve this?	A: GDPR imposes additional obligations on top of other legal obligations, meaning that you cannot use GDPR as a way of getting around other obligations. In the case of the Electoral Roll, under the Church Representation rules there is provision for only the names to be displayed.

	Topic	Question	Answer
	17.6 Electoral Roll	57. Q: As the Electoral Roll officer at my church I am aware that displaying the names & addresses of those on current roll is a current requirement. How is this changed by the introduction of GDPR?	A: GDPR doesn't override any current legislation. The Electoral Roll legislation does permit only the name to be displayed (i.e. address removed), thus protecting people's data. You should not use the Electoral Roll information for another purpose. One good rule of thumb is that there must be "no surprises". Under the "old" Data Protection Act the first company which was fined was a utility company. It allowed a third party to put advertisements inside the bill envelopes. The ICO said people had a certain expectation of privacy. They might expect to be told about local plumbers or to offered a boiler warranty. They would not expect to see an advertisement from a funeral care company. A good rule of thumb under GDPR is to ask would I be surprised to receive this communication? If the answer is yes, you may not have been transparent enough about how you are sharing data.
	17.7 Electoral Roll	58. Q: Is there an issue with making the Electoral Roll publically available during the sign-up period?	A: The electoral roll is covered by church law. GDPR does not override any other laws therefore the electoral roll law still applies. This means that using the electoral roll for is statutory purposes (including public display) does not contravene GDPR. Using the data on the electoral roll for any other purpose would require consent under GDPR.
	17.8 Electoral Roll	59. Q: Should you send out a consent form with the annual electoral roll revision form?	A: Yes if you intend to use the electoral roll data for any other purpose than its statutory uses. Consent must also be renewed every two years.
	17.9 Electoral Roll	60. Q: Why can a consent form not simply be included on an electoral roll form?	A: You should keep the statutory form for the electoral roll separate from the consent form. Instead of combining the two it was suggested that instead every opportunity of providing a consent form be used, including whenever electoral roll forms are given out. It must be clear that the statutory form for the electoral role and the consent form are separate.
	17.10 Electoral roll	61. Q: Electoral roll – can the details on the ER be used for other purposes?	A: No – the ER details can only be used for other purposes if consent is obtained.
18.	18.1 Electoral roll	62. Q: Electoral roll and consent:	A: If we send information to them we must have consent – if they don't respond (e.g. don't return the form) then phone or e mail them to remind them
19.	19.1 Employee contracts	63. Q: My question is about employee contracts and consent in that context.	A: Under current law employees cannot give consent to their data being processed. The new law confirms this position. Consent must be 'freely given' but because of the imbalance of power between employers and employees, employees can't give consent. If you have an employment contract containing a clause which says along the lines of "you give consent to us processing your data", you cannot rely on that clause but you do not need to amend all of your existing contracts. In that case you would use

	Topic	Question	Answer
			the role holder data privacy notice which explains what will happen to the employee's data. For new employees, remember to ensure that any clause referring to consent is no longer in new contracts.
20.	20.1 Fees	64. Q: A further question is about an annual 'data protection fee'. What is this fee for; to who is it payable, how much is it, and do we have to pay it?	A: PCCs will be exempt from the new fee which is £40 for organisations of less than 10 employees and £60 for organisations of up to 250 staff. Larger companies will pay up to £2,900.
21.	21.1 Fines & penalties	65. Q: GDPR is aimed at big business and seems ludicrous when applied to small organisations that don't have IT departments etc. Do we seriously expect that the courts will fine us for sending out the coffee rota?	A : No one can guarantee that a small organisation will not be fined. You are accountable for the data you process. Try to demonstrate that and be transparent. The ICO's view is that the price you pay for processing data is to comply with the GDPR – if you don't want to then don't process data.
22.	22.1 Gift Aid	66. Q: For Gift Aid and Stewardship, presumably you need consent to process their data?	A: The regulator (the Information Commissioner) has an extremely broad view of what is marketing – basically, anything done in furtherance of the interests of the church. If someone withdraws their consent then you cannot contact them again. Remember that consent can be obtained verbally. At a meeting, you might take email addresses and then say that you want to contact everyone to give them details of future meetings and is that ok? If someone says no then you would need to remove their email address from the list. Similarly, if you want to refresh consents and send out the consent form and do not receive a reply you might telephone them and check. Remember to keep a record of having contacted them and the outcome of the call.
	22.2 Gift Aid	67. Q: Is the fact that someone has completed a one-off Gift Aid envelope OK to process their information?	A: Yes, provided that all we do is process it for Gift Aid recovery purposes and do not contact them for another purpose. So, it is ok to write to them at the end of the year with a record of their gifts in the year because this is connected to processing for Gift Aid. However, it is a missed opportunity so think creatively about getting the Consent out there.
	22.3 Gift Aid	68. Q: We are required to keep Gift Aid envelopes for 7 yrs. Do we need to go back to previous donors to remind them that their data has been kept?	A: The suggestion is to use up current stocks of such stationery but amend future versions to include some of the data privacy language (for example on the back of envelope). This could refer someone to the privacy notice available on the church website. If the information is to be used for other purposes, such as raising more funds, then you need a new consent. In summary, it is best to give every opportunity to get consent.
	22.4 Gift Aid	69. Q: Do statutory obligations, say to retain gift Aid records for 7	A: Yes statutory obligations and regulations continue to apply and override GDPR. GDPR

	Topic	Question	Answer
		years, override the right to be forgotten?	doesn't say that you only need to keep data for a certain period but it does say "be transparent"
23.	23.1 Insurance	70. Q: Are there insurance products to protect the PCC against possible fines?	A: The market hasn't really developed yet for GDPR insurance. Part of the issue is the potential for large fines. A market may evolve but at present be wary as any insurance may not offer adequate cover and may have exclusions.
24.	24.1 International transfers of data	71. Q: Is it correct that all data has to be kept within the EU and cannot for instance be held on US based clouds?	A: It's illegal to send data outside the EU unless consent is obtained or some other approved legal means is used. If you buy services or apps there are often two versions of the product – an EU only one and another, often cheaper, version. You usually have to specifically ask for the "EU only" version. Free apps/tools often send data outside the EU – you need to check the T & Cs.
25.	25.1 Legitimate Interest	72. Q: GDPR has 6 legal bases for data processing. Although much of the focus is on consent are there any circumstances in which a newsletter can fall under any of the other bases, for example, legitimate interest?	A: Marketing can be a legitimate interest. However, to rely on legitimate interest as the basis to process data it is necessary to carry out a balancing test and you need to establish your right to carry our direct marketing is more important than an individual's right to privacy. This will be difficult to establish. There are other legal grounds for processing data and the processing might fall under more than one legal basis. For example, there is a legal obligation to maintain the Electoral Roll, but the data on the roll should not be used for another purpose.
	25.2 Legitimate interest	73. Q: Can you use the fact that they are a church-goer as a legitimate interest to cover you instead of getting consent?	A: Legitimate interests include direct marketing, but you would have to establish that the church's right outweighs the individual's right to privacy which will be difficult. Other dioceses are using the consent route instead.
26.	26.1 Newsletters	74. Q: Can newsletters and church magazines/leaflets be sent/delivered to addresses if not selected on the basis of a list of named persons?	A: An address is personal information itself, so a newsletter sent to "the home-owner" by post would still be processing personal data.
27.	27.1 Parish Directory	75. In addition to being the Electoral Roll officer, I also produce a Parish Directory of about 100 names, addresses, telephone numbers, mobile numbers and e-mail addresses. Every year after the APCM I update the Directory, by e-mail (for those with e-mail addresses), telephone calls or talking to people at church. I undertake this task meticulously. Then the Directory is reprinted, named and distributed. No other person who is not in the Directory is given a copy and a note (see below) is attached to each copy.	You do not need to ask them to submit their details again. You could ask them to confirm their details are correct and up to date but this is not necessary, it's just good practice. Using "BCC" is recommended otherwise you are revealing everyone's email address to everyone else.

	Topic	Question	Answer
		<p><i>Here is the updated 2017 Parish Directory so that members of the family of St. Andrews are able to contact each other easily. Compliance with the Data Protection Act means that personal information, particularly e-mail addresses, should not be passed on to a third party without the permission of the person concerned. I update the information rigorously each year and thank you for your co-operation on this matter. Please let me know if you know of any other member of the Church would like to be included in the Directory next year.</i></p> <p>After the APCM this year in April, I will be asking members for their written consent (using the Consent form). The question is - Will I need to ask them to supply their details again (which will cost them a lot more effort and in reality their details are already on file) or can I say: "May I use your details as in last year's Directory and please let me know if there are any amendments?"</p>	
28.	28.1 Pastoral care	76. Q: We also have a pastoral care group who visit elderly/housebound church members as well as those who live in care homes. There is inevitably some sharing of information about those who are visited, for instance in meetings of the pastoral care team. What do you advise about how to take consent for sharing of such information, given that many of the people we deal with are unlikely to have the capacity to give informed consent, and in some cases we don't have contact details for the next of kin.	A: Firstly, be transparent about who you share data with. When collecting information from next of kin you can verbally ask for confirmation that you can add the data to your records, and again be transparent about what you are going to do with the data. One person can give consent for another but the consent has to be specific, informed, unambiguous and opt-in.
29.	29.1 Personal or work email addresses	77. Q: What about email addresses – many people will use either a personal or other work email address for church business?	A: There are 2 points here: how the data is sent and also whether there are other restrictions on using a work email address. Any account which has been used for church business is searchable in the event of a Subject Access Request. Using a work address may be in breach of work policies. Also think about how sensitive data is shared? The key thing is to make sure that there are adequate controls in place. GDPR adds security obligations. This might include password protecting documents. (If data is lost and was not password protected then the ICO would

	Topic	Question	Answer
			consider this as a data breach. Using the same method to communicate the password is also a data breach.) But, why send a document in the first place? If there is any IT infrastructure it is very quick to add the file to a hard drive and send the link by email. IT can also keep records of the IP address of every laptop or computer which accesses the document. If you take these simple steps, your security will be appropriate and proportionate. If not, this might increase a fine if the ICO were to investigate.
30.	30.1 Photos	78. Q: Would displaying photos without any identifying names be included under GDPR?	A: Anything which identifies a living person is personal data. (This can include as little as 3-4 digits of a post code.)
	30.2 Photos	79. Q: How does one monitor photograph content?	A: There are no changes from the current law. Try to be reasonable. Consider blurring subjects who have not given consent. You can also publicise that group events will have photographs and check permissions that way.
	30.3 Photos	80. Q: Is consent needed for using photographs, CCTV?	A: If CCTV is in place there should be notices stating so. For photographs to be used in a prominent way then consent is needed, but e.g. a wide shot photograph of an orchestra is unlikely to require consent.
	30.4 Photos	81. Q: Photographs of people:	A: Photos are personal data and there would need to be consent for individual clear shots. If it's a general congregation shot (or for example a fete) the need to make people aware there is a photographer and give them the opportunity to opt out
	30.5 Photos	82. Q: One website says "Photographs, videos and other media (e.g. audio) in which individuals can be identified can be seen as personal data in the eyes of the law". Is this correct? And if so, what does "identified" mean - does it cover just the image or does it mean an image with text or a caption naming those in the image? If the former (i.e. any image) does this cover church magazines, images displayed on noticeboards, on church websites? Can a person request their image (data) to be deleted, and how does that work out when the photo is a personal photo of a church member used for the church magazine/etc?	A: If you can clearly see someone's face or other identifying features in a photograph then it is personal data. A fuzzy or pixelated photo will not identify them.
	30.6 Photos	83. Q: Can I take and circulate a photo of a troublesome individual to other local churches and internally to protect staff and volunteers even though I don't have his consent to take a photo of him?	If they are troublesome because you think they might commit a crime then you can retain and circulate their data without consent and without notifying them. Be careful about what you say about them in covering emails. Unless a criminal

	Topic	Question	Answer
			offence may be committed, anything you put in an email may have to be disclosed to them.
	30.7 Photos	<p>84. A question about photos of living people.</p> <p>I can see that publishing an individual's photo will need a consent. What is the situation regarding consents for photos posted/published historically?</p> <ul style="list-style-type: none"> - photos on the parish website - photos on social media accounts (Facebook/Twitter/Instagram) eg. a clergy member's private Facebook account. - photos on printed media used by the parish, eg. posters and leaflets 	You do not need consent to publish a photo unless you are publishing it to promote the interests of the parish or church. You should ask for consent if you are going to feature a persons photo prominently.
31.	31.1 Prayers	<p>85. Q: We give out notices which might include requests for prayer, sometimes for non-churchgoers. The notices are also put on the website – how can we comply with the GDPR?</p>	<p>A: There are several ways. If you are collecting details on a form then you could include a phrase such as “please make sure you have got consent to provide this person’s information”. If you do this then you can rely on the completed form. You could take a risk based approach/ For example, how likely to complain is the person being prayed for? If you are not sure about consent or it cannot be obtained, then perhaps you could include the person in silent prayers rather than naming them. There is no need to mention the illness. This is likely to be sensitive personal data.</p>
	31.2 Prayers	<p>86. Q: What if someone asks for a neighbour to be prayed for? Is this ok?</p>	<p>A: Has that neighbour given their consent? <u>If</u> the person who is requesting the prayers does not know then it <u>might</u> be appropriate to pray silently but without mentioning the neighbour by name. It is, however, important that the illness should not be made public, unless the consent to share this information has been expressly given.</p>
		<p>89a. As a Hospital Church we have people leaving prayer requests on our prayer board in the expectation that these will be read out at one of the Sunday Eucharists. People specifically come to the Eucharist, knowing that their loved one is being prayed for then – what is the situation regarding GDPR and public prayers?</p>	<p>As the national guidelines say, where personal data (such as information about health) is going to be recorded and published, such as on a church website or in a newsletter, it is good practice to ask the person concerned whether they’re happy for that to happen.</p> <p>Obviously there is room for pastoral judgment here. In sensitive situations in which somebody is highly likely to be unhappy about having their name and/or other information shared, we do advise seeking their agreement, and refraining from sharing their information in print where consent can’t be obtained.</p>

	Topic	Question	Answer
			This is not a new issue. Under the existing Data Protection Act, passing on (in a 'written' form) sensitive personal information about someone without their consent is in breach of the guidelines.
	31.3 Prayers	87. Q: Elsie is worried about Florence who doesn't come to church. Elsie lights a candle and adds a note which says that Florence is ill with cancer. Is this ok?	A: It is ok to give names but not details of the illness as this is sensitive personal data. However, you also need to try to ensure that consent is obtained, particularly in our multi-cultural society where people may object to being prayed for. You could ask Elsie to ask Florence for consent. Alternatively, Florence could be prayed for through silent prayer. But there is no need for the illness to be known or shared, except with someone if they were going to be making a pastoral visit.
	31.4 Prayers	88. Q: Continuing with Florence & Elsie. We have quite a list of Florences mentioned on the church newsletter each week. Do we need to contact all of them for consent?	A: The best thing is to ask the Elsies to get consent. You could try putting a notice in the newsletter to say that this needs to be checked going forward. Remember (a) it is really not necessary for everyone to know why they are ill and (b) GDPR applies to all EU nationals & residents.
	31.5 Prayers	89. Q: Still with Elsie & Florence. How do we proceed if Florence is too ill in hospital to give her consent but Elsie really wants Florence on the prayer list.	A: It would be a good idea to ask Elsie if Florence might mind. By asking Elsie this will at least get her thinking about it.
	31.6 Prayers	90. Q: Is there a problem with strangers naming other strangers on the prayer board?	A: No but you should put a notice up saying that permission should be sought before adding someone's name to the board.
	31.7 Prayers	91. Q: How should we handle requests for prayer? We have a prayer board in church where people write up names of people to be prayed for, and historically those names (nothing more) have been printed in the weekly newssheet. It's an important aspect of parish life that people feel that they can pray for each other and be prayed for by name, but how do we handle this in this new climate?	A: The important question is handle them sensitively. You could put a sign up stating that parishioners can add names but you do not need to know the illness or reason for the prayer. You could also pose the question – does the person know they are being prayed for? Would they mind? It might prompt your good-natured parishioners to think about this before offering a name.
32.	32.1 Privacy Notices	92. Q: In the first section of the privacy notices there is a passage enclosed in [] and written in italics, thus: The processing of personal data is governed by [the Data Protection Bill/Act 2017 the General Data Protection Regulation 2016/679 (the "GDPR" and other legislation relating to personal data and rights such as the Human Rights Act 1998)]. This is very unclear (and there is a missing closing bracket). It gives a date of 2016 for this new	A: The correct reference for the GDPR is "2016/679" as it was written into the EU statute books in 2016 and not 2018. Confusingly there will also be soon a Data Protection Act 2018 which you should also refer to.

	Topic	Question	Answer
		legislation, which can't be right. I propose in our customised document to write: 'The processing of personal data is governed by the General Data Protection Regulation 2018 (GDPR), and other legislation relating to personal data and rights such as the Human Rights Act 1998.' Would I be correct to do this?	
33.	33.1 Retention Periods	93. Q: How long do the consent records have to be retained?	A: Each church should have a consent policy and keep the records in line with this. The ICO have said that consent does have a shelf life (of around 2 years) so will need to be renewed every couple of years. On data privacy, the suggestion is to keep the data for at least 7 years as this is uniform across lots of categories within church record-keeping.
34.	34.1 Right of erasure / right to be forgotten	94. Q: Does someone have the right to be deleted from PCC minutes?	A: If there is a legal reason to keep the data then you do not have to delete it. You must communicate your decision and reason for keeping the data within the one calendar month time limit.
	34.2 Right of erasure / right to be forgotten	95. Q: Is there a way of proving deletion?	A: Delete the data and then try to search for it in the same way that you would were there a Subject Access Request.
	34.3 Right of erasure / right to be forgotten	96. Q: Are there exceptions to the Right to be forgotten?	A: Yes, legal obligations to retain data or legitimate interests may override a request to be forgotten. If there is a sound legal reason to retain data, it does not have to be erased.
35.	35.1 Role holders	97. Q: Role holders – would this include sidesmen?	A: Yes. Issue them with a role holders privacy notice.
	35.2 Role holders	98. Q: I am also unclear about how we deal with role holders for whom not all information we hold is directly related to their role. Taking the example of our pastoral care team members, I can understand that we cannot rely on consent for holding safeguarding information about them. But if, for example, we want to email them about forthcoming events in other aspects of church life, or include them in the Church Members' Directory or their birthday in the newssheet, do we need to obtain a consent form for those uses?	A: Role-Holders may well have a dual role. They may well participate or give gift-aid donations. We recommend sending them or giving them both privacy notices.
	35.3 Role Holders	99. Please would you clarify the two following queries regarding Privacy Notices. To non-role holders As the only action required, would it be appropriate just to display a hard copy on the internal Church Notice	You should make the non-role holders notice available on your website and draw attention to it in newsletters and emails. For the role-holders notice, you can edit this and remove the data you will not keep but then you should send it to all role holders.

	Topic	Question	Answer
		<p>Board and on the Church website via a link?</p> <p>To role holders In addition to the ones mentioned (PCC Treasurer, PCC Secretary, Deanery Synod Reps, Safeguarding Officers), we have numerous other members who hold lists, such the cleaning rota, coffee rota, Bible readings, Messy Church, Uniformed organisations (which are church groups), Language Club, Servers and several others.</p> <p>Do all these role holders need a copy of this Notice, which in itself can be viewed as intrusive and could be misread as a requirement, eg gender, employment details, passport numbers, driving license numbers, tax reference numbers. I know the Act needs to cover all eventualities but these details would not normally be held by churches.</p> <p>In addition, there is no direction in this Privacy Notice to the role holders that they need to obtain written consent from the people on their list as no central lists are held. An appropriate Consent Form could be supplied by the PCC (ie the person deemed to be in charge of Data protection) and this could be distributed to all role holders for onward distribution to members on their list; in this way it would ensure that nobody is missed. Would the Consent Forms need to be held centrally, say in the Church office, which would minimise the number of holding places. I am asking this so that we can proceed correctly and advise members accordingly.</p>	<p>The notice informs role-holders about how their data is processed – it is not designed to give them instructions on how to obtain consent or process other people’s data. You should do this through training the role-holders/</p> <p>Yes the consent forms should be held centrally.</p>
	35.4 Role holders	100. Q: How do you determine who is a role-holder? We have people involved in church activities – does that make them role-holders?	A: Yes. Remember that you might have people with dual roles so they could require both types of privacy notices.
36.	36.1 Safeguarding	101. Q: In terms of safeguarding and allegations made does the issue of consent go away?	A: Safeguarding is a legal requirement and therefore consent is not relevant.
	36.2 Safeguarding	102. Q: I am the Safeguarding officer for my church. Occasionally I might get sent something by our Youth Worker who will explain a situation (anonymised) but	A: You don’t need to get consent from the young person. It is important to keep processing this kind of data but you might think about keeping it securely. Don’t use GDPR as an excuse to stop doing very good work.

	Topic	Question	Answer
		someone could still identify the relevant individual if they then look at the youth group. It isn't notifiable even to the Diocese, although I would share the broad details with the Rector. I then keep the email and wait. What do I have to change going forward?	
	36.3 Safeguarding	103. Q: Does GDPR over-ride safeguarding concerns?	A: No, GDPR should not prevent proper safeguarding.
37.	37.1 Scope of GDPR	104. Q: Where would you draw the line in respect of personal activities undertaken versus activities which the parish undertakes – for example, if people are going out initially as part of a food bank initiative but are encouraging people to come to the church at the same time.	A: Think about if they are doing it on behalf of the parish or not – if they are doing it for themselves then they wouldn't need the role-holder privacy notice.
	37.2 Scope of GDPR	105. Q: As a Lay Reader I come across all sorts of information about people, some of which is written down and some is kept in my head. My motivation might be to find ways to involve people in the church. How much is this legitimate to keep? And would a verbal consent be ok?	A: Yes, verbal consent is ok. It might start as a fairly narrow consent for one thing but widen over time. So, they might have expressed interest in a particular thing but you have then thought what about other activities. When they come to church you could give them the general consent form and offer an opportunity to be more involved. The draft Consent Form in the GDPR Toolkit has several layers: a) We will send you a newsletter, b) We will ask you to get involved, c) The third level is a blank box to add activities which might be relevant to your church. In respect of this third level it would be helpful if you also let the Diocese know about them in case if it appropriate to amend the Toolkit.
	37.3 Scope of GDPR	106. Q: If a member of staff has left the parish, for example, a cleric, and they took some data with them are we responsible for getting them to get rid of all of that data?	A: Yes. So before they leave you need to get them to do some data cleansing. The reason for this is that if there is a Subject Access Request you need to check all locations where anything is stored. Don't forget, using work email address for a voluntary role would also be covered by a Subject Access Request. (As well as possibly also being in breach of work policies.) Also, check information you have on social media.
	37.4 Scope of GDPR	107. Q: As a priest I am personally covered by GDPR. But when I go home at night I don't stop being a priest. I have a certain amount of personal data at home, as well as at work.	A: The use of a contact list for social and domestic purposes is not covered by the legislation. Using personal data in a professional capacity is covered. So ministering to a parishioner in the current parish will be covered by GDPR. In the Church of England there are many joint data controllers and all are jointly liable and jointly responsible.
	37.5 Scope of GDPR	108. Q: In a Parish there are a number of people involved with sensitive information and a wide range of opinions – how can we get compliance from everyone given the group liability?	A: The starting point is to raise awareness so that everyone is on board. If you think that staff are a risk take steps to limit this (such as switching off the address auto-fill capacity in Outlook). Think about the confidential waste bag left unattended which becomes a lucky dip to

	Topic	Question	Answer
			anyone who can access the place where it is stored. Think about physical security as well as electronic security.
	37.6 Scope of GDPR	109. Q: Personal data – does this exclude companies?	A: Yes it does but you may have the names of individuals. Consider the risks – are they likely to complain if you keep their data. There needs to be clauses in contracts to cover this.
	37.7 Scope of GDPR	110. Q: Are the pastoral care notes which clergy keep covered?	A: Yes and they would be caught by an SAR unless there is a legal exemption. There may also be a need to redact to avoid disclosing someone else's personal data when answering a subject access request. Care is required over redaction – don't use an electronic means and then just email the document as it is possible to undo the redaction. You need to do the redaction, then print off the document and scan in the redacted document. If you use a pen to do the redaction make sure it cannot be erased or be seen through and again photocopy the redacted version and either send the copy or scan it and email it. People have a right to the information in the documents, not to the document itself.
	37.8 Scope of GDPR	111. . Q: What about youth ministers etc using Instagram – does this fall under GDPR	A: Yes it does
	37.9 Scope of GDPR	112. Q: In a church context where is the boundary between ministry and friendship? E.g. one person gives their phone number to someone else and they pass it on	A: GDPR doesn't apply to personal information held by people as individuals (i.e. friends) so people need to be clear on what basis they have obtained the data.
	37.10 Scope of GDPR	113. Q: The GDPR is for organisations and businesses so I am assuming that individual (self-employed) Spiritual Directors do not have to conform to these new rules? I would appreciate your clarification.	A: If a spiritual director is acting for or on behalf of a data controller such as a bishop or PCC, the bishop or PCC will be responsible for their actions. The spiritual director may not be an independent data controller because of the way they are operating.
38.	38.1 Security	114. Q: Is it OK to keep information at home?	A: Wherever it is kept it is a PCC liability. E.g. CVs for organists, administrators being kept at PCC member's home. An audit of what info is kept where, would have flagged this up.
	38.2 Security	115. Q: What is the best way to protect information e.g. password protect email documents (with password sent in separate way e.g. text, phone)	A: Yes. Do not send a password protected email and the password by email. You should text the password. Inadequate security measures can lead to greater fines.
39.	39.1 Sharing data	116. Q: As far as I can see, the way that the current consent form and general privacy notice are drafted, they do not provide for the sharing of personal information among church members in any way, but are limited to enabling 'the church' to communicate directly with the data subject. To take a couple of examples in our parish, we have a	A: You should adapt the privacy notice to include information of everyone you share the personal data with.

	Topic	Question	Answer
		weekly newssheet which will include personal information such as birthdays and we circulate the contact information for everyone on our rotas to everyone else on the rota so that, for example, people can arrange swaps between themselves. We also issue an annual 'Church Members' Directory' where (with specific consent) members' contact details are circulated to each other. I suspect that the majority of churches will do similar things. What advice do you have about this, and I wonder whether this should be specifically covered in the templates offered to parishes by the diocese?	
40.	40.1 Subject Access Request	117. Q: Subject Access Request – if it's a safeguarding matter what do I have to disclose (e.g. do I need to disclose speculative information?)	A: Yes you will need to disclose all information but care will be needed to avoid disclosing anything which would identify the accuser or anyone else's personal information. If the details of the allegation would by implication identify the accuser then it needs to be redacted. If in doubt err on the side of caution and redact in safeguarding matters.
	40.2 Subject Access Requests	118. Q: Under a Subject Access Request would this kind of information (from previous question about safeguarding) need to be disclosed even though it was anonymised?	A: You must disclose anything which is clearly identifiable. A Job description might be enough to identify someone. Or, in some parts of the country, a part of the postcode might do so. Remember, all of the exemptions from the Data Protection Act have been transferred across to the Data Protection Bill (for now).
	40.3 Subject Access Requests	119. Q: What about fees for subject access requests?	A: A search of historic registers carries a fee; but a SAR does not. We may see a rise in SARs as a way of avoiding the search fee.
	40.4 Subject access requests	120. Q: Subject access requests – what third party information is covered?	A: Anyone you have a contract with. Volunteers using home and/or work e mail addresses are all searchable. Some workplaces have an e mail policy prohibiting their use for "personal non work matters". If work email addresses have been used by a volunteer they would have to be searched if an SAR was received.
41.	41.1 Third parties	121. Q: When we rent out our spaces we have to ask hirers to be compliant with our safeguarding policy – is it the same for GDPR – do we have to ask them to comply?	A: If you have no access to the data held by the hirer then there are no obligations on you. But, it is good practice to ask them to be compliant with the GDPR.
	41.2 Third parties	122. Q: When we arrange funerals we will receive next of kin data. Can we keep this information to use to invite them to relevant services or other activities?	A: It can be used for the purpose it was given for - anything further would require consent. Think about if the use might give cause for them to complain. You don't have to be over the top with the language, alternatives words may get to the same answer.
42.	42.1 Training	123. Q: legal obligation to offer training – do PCCs have to offer	A: Yes – Diocese training will count but the PCC will also need to offer training (e.g. the online

	Topic	Question	Answer
		training or just relay on the Diocese training	training) and keep a record. Training needs to be on-going.
	42.2 Training	124. Regards GDPR training - we have 22 in the PCC, does each person have to be trained? I understand that data processing role-holders, clergy, staff, volunteers have to be trained.	Yes everyone who handles personal data should really be trained.
43.	43.1 Voice recordings	125. Q: Are voice recordings covered?	A: Yes. If there is a Subject Access Request which includes a voice recording then you can redact other people's personal data by either a) recording white noise over other people's data or b) by typing out a transcript and blacking over other people's data. NB When people submit a Subject Access Request they are entitled to know what information you hold on them but they do not have the right to see the documents.