Photos

1. For public events such as church services do we have to haver consent to use photos we have taken?
2. Do we need to have model release forms signed for any photographs we take at events?
3. Does whether or not we name people in photos make a difference?
4. If I am asked to take pictures and video at a church event, just by turning up have people given some sort of permission for this?
5. If the material is to go on social media or website do I need signed permissions?
6. Do I need to give an undertaking as to how long the data will be stored?
7. I would like to include photographs of a recent event in the parish newsletter. Do I need to get consent for this?

Who's responsible?

8. We have a 'friends of …' group. This is run separately to the church PCC, but they fundraise for us. Is it correct that the friends group will sort out their own data protection?
9. Is it true that the PCC and incumbent will be considered as separate entities under this legislation requiring separate data control?
10. I work for a parish. By storing the data on my own computer, ipad, phone am I putting myself as a separate entity under the law?
11. Is the phrase "incumbent or priest-in-charge", being used generically, i.e. for all ministers, or specifically for those of incumbent status? If generically then all ministers, whether incumbent, associate priest, curate, reader lay pastoral assistant etc. are data controllers and each will have to be able to demonstrate that they are complying with the GDPR. If "incumbent or priest-in-charge" is being used in the legal sense then who will be the data controller for the data that colleagues hold, the incumbent or the PCC?
12. Who is the data controller for parish information?
13. Is a multi-parish benefice or cluster a single data controller?
14. Who will be the data controller for data that the "incumbent or priest-in-charge" holds? Who is responsible for compliance in the Diocese?
15. What are the implications of the incumbent being a separate data controller?

Data you hold

16. Are there any issues with visitor books?
17. We store names and addresses both on computer and envelopes for claiming Gift Aid – How long after a regular giver stops paying should we keep the donation record? Similarly a one off giver e.g. holiday maker how long since the last donation or claim?
18. We hold information about children and young people who attend activities at our church, is this ok?
19. How long do I need to keep information for?
20. Do copies of funeral visits / notes, funeral director confirmation letters, sermons etc need to be shredded or can they be kept as they contain contact details for next of kin?

21. At every funeral we receive from the undertaker the 'green form' from the Coroner/registrar or whoever is appropriate to approve the burial/cremation of the deceased person. The bottom of the form is them torn off, signed and returned to the registrar. The information on the top part of the green form is written into the burial book at the time of the service but we don't know if we should keep the actual form itself once this procedure has taken place as it is duplicating what we already have.
22. Do we keep copies of personal details forms and confidential declaration forms once an applicant has had a DBS check done?
23. Under the GDPR individuals have a "right to be forgotten", i.e. a right to have their personal data deleted. We have some historic information relevant to an allegation made against a former clergy person. Can that individual exercise their right to be forgotten and require us to delete their personal data?
24. Can we keep personal data for historical research purposes without consent?
25. Safeguarding advice appears to be – keep everything. A diary or parish magazine from twenty years ago can show that someone was not where it is alleged they were, or was not a churchwarden when they claimed to be. Is this in conflict with the right to be forgotten?

Consent

26. We will be issuing a reminder at our APCM tomorrow evening but I am concerned that those who have not returned the forms to date may not do so. As I understand it, without consent to contact them we will be unable to inform them when the ER is replaced next year. Is this correct?
27. Can I use contact details obtained from the electoral roll to contact people with Church news and events?
28. We are required by the CRR to post the electoral roll on the door of the Church for 3 to 4 weeks before the Annual Parochial Council meeting. This list includes the name and address of each member of the congregation/parishioner on the list. What are the implications on this vis a vis the Data Protection Act? And can we legally post such information in a public place, ie the main door of the Church?
29. Should every member who agrees for their information to be on a congregation contact list sign a separate consent form?
30. How we can continue to keep up-to-date pastoral notes on the elderly folk that we visit/have contact with in care homes etc and who have memory problems/other illness which means that we are unlikely to be able to get informed consent from them to continue to hold this information.
31. We hold "in case of emergency" contact details (usually a name and phone number) for members of our church family's next of kin, will we need to also have THEIR permission to hold THEIR names and phone numbers on our database, as well as the permission of the member of the church family?
32. Do we need consent to communicate with people about giving.
33. Will Church House Publishing or SPCK be updating their standard forms for baptism applications and wedding banns to include consent for the Church to inform them about upcoming consents?
34. What is the position about weddings / baptisms / funerals from past years? I guess we can send baptism anniversary cards and Christmas cards to wedding couples

provided it is simply that, if we use it to advertise or fund raise then presumably we will need consent?

35. I have contact details for family members which I have obtained through funerals, weddings, baptisms and so on. Do I need consent before I contact them about events? Also, do I need consent before sharing their contact details with other vicars?
36. Currently, material is frequently sent home with children promoting events at church that have nothing to do with school life. Do our schools now have to obtain the express permission of parents to communicate with them about church rather than school affairs? The Diocesan vision wishes us to consider our schools as an extension of our worshipping communities but these regulations appear to work in precisely the opposite direction.
37. Can parents give consent on behalf of their children for GDPR purposes?
38. We often send out named invitations to the whole village to attend special services. Can we do this without specific permission?
39. Can the Church discuss in person with parishioners who are not necessarily regular church attenders about the Parish Giving scheme?
40. When do we not need consent to process special categories of personal data (such as information about religion)?
41. What does "consent" really mean in practice? Does it have to be in writing? Also, can consent be implied (for example, we have been sending parishioners newsletters for years, can we treat it as valid consent if they have never opted-out or complained)?
42. We send a Benefice Magazine to every household in the benefice which advertises Benefice Church events and also has advertisements from local or relevant traders. Should we be getting consent to deliver this before we push them through people's letterboxes?
43. Do we need consent before sharing information about people who help out in the Parish? For example, we give flowers to comfort people (eg, if they are bereaved) every Sunday. We have a rota so that volunteers know when they are on duty. Do we need to get consent from a volunteer to share the rota with other volunteers?
44. Do we need to get all of our existing consents with people renewed?

IT and security

45. Is the home computer secure enough - are we falling foul of any rules?
46. Is it ok for me to use an online document storage system, for example Google Drive or Dropbox?
47. I understand that under data protection law we need to make sure that the personal data we have is kept secure. This is not something I have thought about before. Where do I start with this?
48. I need to enter a password before I can access the start screen on my laptop. Does this count as encryption?
49. We have lost a laptop containing staff and payroll information. The laptop also contained scanned copies of staff employment contracts. The laptop was not encrypted. Do we need to tell anyone?
50. I have heard a lot in the news about cyber threats and organisations being hacked. Is this relevant to our parish?
51. Can our volunteers use personal or work email addresses?

52. What do I do about the email addresses that my email system remembers and autocompletes?

Sharing data

53. How can we continue to provide good, team-based pastoral care in these circumstances, especially where different members of the team may visit/receive updates, and where visits are less frequent (and therefore especially important to have written 'memories' of what happened/was discussed/etc on the previous visit)?
54. Can we put up a list of our electoral roll members or the Parish officers, including their contact details, on our notice boards?
55. A local charity has contacted us because they are looking for volunteers. We think that a number of our own volunteers would be a good fit for the charity. Can we pass on their details to the charity?
56. Once people have agreed to be in the directory/congregation list, which we currently only give to people in the directory/ congregation list, with say 200 copies distributed it is virtually impossible to ensure that it won't be shared, even if you print on the directory that the information in it may not be shared with anyone not included.
57. Can we still send details of deanery synod elections and churchwardens elected etc. to the diocesan office. Will we need consent to do this?
58. My parish is in a multi-parish benefice – how do the consent and privacy forms relate to that situation rather than the single parish/benefice situation?
59. We have paid staff and the payroll is provided by another organisation (e.g. a diocese or payroll service provider) – can we still share information with them?

General

60. Do I need to register us with the Information Commissioners Office (ICO)?
61. What is a privacy notice?
62. How do I go about providing a privacy notice?
63. Who do I need to provide a privacy notice to?
64. How do I recognise a subject access request?
65. When do I need to carry out a data protection impact assessment?
66. Do we need to complete a data audit?
67. I would like to collect information about parishioners even though I am not yet sure what I want to do with that information. For example, we are thinking about new events and activities to improve engagement but we don't have any fixed plans yet. What do we need to do?
68. What do I need to do to make sure that the information we have is accurate?
69. Should I report a data breach and when should I do it?

Photos

1. For public events such as church services do we have to haver consent to use photos we have taken?

What are you doing with photo? If using on a place such as a website yes unless you have another legal lawful basis.

2. Do we need to have model release forms signed for any photographs we take at events?
   Yes for individuals. Its common practice. You could add it to your usual consent form perhaps.

3. Does whether or not we name people in photos make a difference?
   Yes.

4. If I am asked to take pictures and video at a church event, just by turning up have people given some sort of permission for this?
   No.

5. If the material is to go on social media or website do I need signed permissions?
   If individuals yes. It is wise to do so. You may elect to ask before taking a picture, you need a record of this consent.

6. Do I need to give an undertaking as to how long the data will be stored?
   Have a privacy policy on your website that explains how you use photos.

7. I would like to include photographs of a recent event in the parish newsletter. Do I need to get consent for this?
   Yes, you will need to do so in the vast majority of cases. For children, the consent should come from the parent until the child has reached 12. Once they are 12, the consent should come from the child and the parent. Once they are 16 or over, the consent just needs to come from the child.

Who's responsible?

8. We have a 'friends of …' group. This is run separately to the church PCC, but they fundraise for us. Is it correct that the friends group will sort out their own data protection?
   Yes, if they are not part of your legal entity.
9. Is it true that the PCC and incumbent will be considered as separate entities under this legislation requiring separate data control?
   Yes
10. I work for a parish. By storing the data on my own computer, ipad, phone am I putting myself as a separate entity under the law?
    You are acting as a processor for the church so not acting as a separate entity and you need to ensure the data is accessible by church should you leave or at least passed over / erased if you leave. You need to take safety precautions such as passwords and potentially encryption. You need to adhere to the Data Protection Policy and commitments of the Privacy Notice.
11. Is the phrase "incumbent or priest-in-charge", being used generically, i.e. for all ministers, or specifically for those of incumbent status? If generically then all ministers, whether incumbent, associate priest, curate, reader lay pastoral assistant etc. are data controllers and each will have to be able to demonstrate that they are complying with the GDPR. If "incumbent or priest-in-charge" is being

used in the legal sense then who will be the data controller for the data that colleagues hold, the incumbent or the PCC?
An incumbent is a data controller. Those in Team Vicar, priest-in-charge and other self-supporting clergy will come under the remit of the PCC as a data controller as well as the incumbent as part of their own individual data responsibilities will also be responsible for ensuring that data shared about individuals eg funerals, weddings etc is held appropriately. All other individuals (pastoral workers etc) in a parish holding data about individuals do so in their roles/ministry in the wider parish and ensuring they are compliant rests with the Incumbent (for good practice and leadership) and the PCC.

12. Who is the data controller for parish information?
The PCC and the incumbent are separate data controllers. They are each responsible for the data they hold and use.
13. Is a multi-parish benefice a single data controller?
Each parish will be a separate data controller. You should make sure that your privacy notice and consent forms make it clear that you are processing the data on behalf of multiple parishes. In addition, you should have a data sharing agreement between the parishes which documents the rules around sharing data, for example, which parish is responsible for the privacy notice and consent form, who responds if an individual makes a complaint or subject access request and so on. The agreement does not have to be formal, for example, an exchange of emails or a letter signed by each parish would be fine so long as the email / letter covers all points.
14. Who will be the data controller for data that the "incumbent or priest-in-charge" holds? Who is responsible for compliance in the Diocese?
The data controller is the person (or organisation) who is legally responsible for data protection compliance. They decide the manner in which and the purposes for which the personal data are processed. Often there will be more than one data controller. For example, if both the incumbent and the PCC use a set of personal data about parishioners then both will likely be a data controller of that information.
15. What are the implications of the incumbent being a separate data controller?
We suggest that incumbents should be thinking about the following in particular: (1) Making sure that privacy notices and consent forms cover incumbents (in addition to the PCCs); (2) Documenting how personal data is shared between them and the wider Diocese. We suggest that there should be some form of agreement in place between the incumbent and the PCC setting out key data governance issues such as who is responsible for the privacy notice, what happens if a data subject makes a complaint or seeks to exercise any of their rights, and so on. The agreement does not have to be lengthy or particularly legalistic. A letter or exchange of emails would suffice so long as it covered the key points.

Data you hold

16. Are there any issues with visitor books?
    It contains personal data so should be at least acknowledged. You need to determine risk. What data do you capture and why? If it is only name and town or country it is low risk, avoid asking for any other personal information.
17. We store names and addresses both on computer and envelopes for claiming Gift Aid – How long after a regular giver stops paying should we keep the donation record? Similarly a one off giver e.g. holiday maker how long since the last donation or claim?
    You need to determine this according to the guidance for data retention. HMRC ask that you keep records for 6 years plus the current tax year.

    The Church of England Guidance 'Keep or Bin' helps advise on this:

    https://www.churchofengland.org/sites/default/files/2017-11/care_of_parish_records_keep_or_bin_-_2009_edition.pdf

18. We hold information about children and young people who attend activities at our church, is this ok?
    Yes. It is in their vital interest to have basic details including emergency contact details. If you wish to communicate with the child, e.g. to tell them about what's on, you will need consent for those under 16 from a parent or guardian.
19. How long do I need to keep information for?
    Guidance on specific retention periods can be found here:
    https://www.churchofengland.org/sites/default/files/2017-11/care_of_parish_records_keep_or_bin_-_2009_edition.pdf

    Please note that this guidance will likely need to be updated to take account of GDPR. The Independent Inquiry into Child Sexual Abuse (the Inquiry) (formerly the Goddard Inquiry) has issued retention instructions to a range of institutions regarding records relating to the care of children.

    In light of this, many institutions are temporarily ceasing the routine destruction of those records which might be relevant to the Inquiry in case they are requested by the Inquiry or made subject to a disclosure order. This means that before destroying any document you should consider if it contains information that may fall within the Inquiry's remit. The range of documentation which might need to be kept is wide. Accordingly, we suggest you seek advice from Church House before destroying any records, this is the case even if the retention period contained in the guidance referred to above has been reached.

    a) For children's activities – the simple details of where there were Sunday Schools, holiday clubs, choirs etc = 50yrs after the activity has ceased

    b) Where there were safeguarding records relating to concerns raised or any risk assessments etc = 70yrs after the last contact with the individual.
    (The diocese could retain these records for a PCC but a separate agreement about records storage will need to be agreed and a PCC minute of what has been agreed so that there is always clarity of access).

c) Personnel files for employees (or volunteers where these are available) for anyone working with children or vulnerable adults = 75yrs after employment. (The diocese could retain these records for a PCC but a separate agreement about records storage will need to be agreed and a PCC minute of what has been agreed so that there is always clarity of access).

d) Application forms for those not successful at application stage =1yr after the role has been filled. Then the form should be shredded and destroyed.

20. Do copies of funeral visits / notes, funeral director confirmation letters, sermons etc need to be shredded or can they be kept as they contain contact details for next of kin?
    You can keep this information so long as you have a good reason to do so. It is of course fine to keep notes of funeral visits so that you can prepare the sermon and also going forward if you need to keep notes as part of ongoing support to the family. The key is that you must be transparent so that people understand why their data is being kept. You could therefore have an explanation in your privacy notice or in an information leaflet made available to the family which cross refers to the privacy notice.
21. At every funeral we receive from the undertaker the 'green form' from the Coroner/registrar or whoever is appropriate to approve the burial/cremation of the deceased person. The bottom of the form is them torn off, signed and returned to the registrar. The information on the top part of the green form is written into the burial book at the time of the service but we don't know if we should keep the actual form itself once this procedure has taken place as it is duplicating what we already have.
    In the guidance from the Church of England (https://www.trurodiocese.org.uk/resource-collection/gdpr-data-protection/) it states that parishes must keep registers of baptisms, marriages and burials forever (they can be deposited at the County Records Office). You may keep registers of blessings and funerals. You should dispose of certificate counterfoils and applications for banns, baptisms and weddings. Given that you will be keeping the information from the green form on the register you do not neaed to retain it (as it is, as you state, a duplication). As you know, you keep the register permanently. You might like, for administrative purposes to retain the green form to inform your reporting and accounting and then dispose of them securely.
22. Do we keep copies of personal details forms and confidential declaration forms once an applicant has had a DBS check done?
    No all these should be sent to the diocese for confidential shredding. The personnel forms should have a recorded, date, outcome and when any rechecks are due, and any personnel information recorded including any capability, disciplinary, safeguarding concerns etc and kept in accordance with the data retention guidelines.
23. Under the GDPR individuals have a "right to be forgotten", i.e. a right to have their personal data deleted. We have some historic information relevant to an allegation made against a former clergy person. Can that individual exercise their right to be forgotten and require us to delete their personal data?
    The right to be forgotten is subject to a number of exemptions. For example, you do not have to comply with a request if you have a legal obligation to keep hold of the information, or if you need the information to defend a claim. In addition, you

can likely keep the information if doing so is in the public interest, this will likely apply in many cases where historical allegations have been made.

24. Can we keep personal data for historical research purposes without consent?
    The short answer is yes although the GDPR requires certain safeguards to be put in place. In addition, individuals have a right to object to their personal data being kept for historical research purposes.
25. Safeguarding advice appears to be – keep everything. A diary or parish magazine from twenty years ago can show that someone was not where it is alleged they were, or was not a churchwarden when they claimed to be. Is this in conflict with the right to be forgotten?
    "The right to erasure", also known as the right to be forgotten, in the GDPR is the right to request the erasure of personal data in certain limited situations, such as where the personal data is no longer necessary for the purposes for which it was collected or processed or where the data subject withdraws consent to the processing, where consent is the legal basis relied upon to process the personal data. Therefore, all personal data that can be legitimately held will continue to be so, unless and until one of the provisions permitting erasure of personal data under the GDPR applies, (such as the purposes for which it is being processed have ceased (or consent withdrawn, (where relevant) etc.). The Independent Inquiry into Child Sexual Abuse (IICSA) has certain statutory powers under the Inquiries Act 2005 and using its statutory powers it has already stated that we should not destroy any personal data that might be relevant to the inquiry and the ICO has agreed this too.
    Secondly, with regard to material, such as the parish magazine, which is already in the public domain the so called "right to be forgotten" will be irrelevant because the material in question is already publicly available. Indeed, it would be completely impractical to request individuals destroy material, such as parish magazines, that has been made publicly available.

Consent

26. We will be issuing a reminder at our APCM tomorrow evening but I am concerned that those who have not returned the forms to date may not do so. As I understand it, without consent to contact them we will be unable to inform them when the ER is replaced next year. Is this correct?
    No, you can contact members of the electoral roll for this reason. This is something that the GDPR allows churches to do.
27. Can I use contact details obtained from the electoral roll to contact people with Church news and events?
    The electoral roll information cannot be used to contact individuals with Church news or events, unless the individual has consented. As a general rule you can send people information about news and events by post so long as: (a) you have been transparent with them (eg, you tell people in your privacy notice this is what you plan to do); (b) it is within their reasonable expectations that they will be contacted in that way; and (c) they are someone who is a member (or former member) of the parish or someone you are in regular contact with. However, in the vast majority of cases you would need consent before sending news and events related communications by email.

28. We are required by the CRR to post the electoral roll on the door of the Church for 3 to 4 weeks before the Annual Parochial Council meeting. This list includes the name and address of each member of the congregation/parishioner on the list. What are the implications on this Vis a Vis the Data Protection Act? And can we legally post such information in a public place, i.e. the main door of the Church?
    The electoral roll information cannot be used to contact individuals with Church news or events, unless the individual has consented. As a general rule you can send people information about news and events by post so long as: (a) you have been transparent with them (eg, you tell people in your privacy notice this is what you plan to do); (b) it is within their reasonable expectations that they will be contacted in that way; and (c) they are someone who is a member (or former member) of the parish or someone you are in regular contact with. However, in the vast majority of cases you would need consent before sending news and events related communications by email.
29. Should every member who agrees for their information to be on a congregation contact list sign a separate consent form?
    They should know they are on the list and how and why the information will be used. Consent is ideal but one assumes these are all church members so you can use the information to maintain membership records.

    A separate issue is where and how the list is shared. If it is used for other purposes then you will need consent, e.g. mailing out about upcoming events.

30. How we can continue to keep up-to-date pastoral notes on the elderly folk that we visit/have contact with in care homes etc. and who have memory problems/other illness which means that we are unlikely to be able to get informed consent from them to continue to hold this information.
    If they have someone with a power of attorney, e.g. a carer, they are able to give consent but this may not be necessary. You are keeping information for which there is a legal basis.
31. We hold "in case of emergency" contact details (usually a name and phone number) for members of our church family's next of kin, will we need to also have THEIR permission to hold THEIR names and phone numbers on our database, as well as the permission of the member of the church family?
    No. You can hold that. Just be careful to ONLY use that in emergencies. Your legal basis would come under vital interest (protecting someone). Encourage them to tell relatives that they are an meemergency contact and the relative would be entitled to know you have it if they ask and to know who has access to it and how secure it is.
32. Do we need consent to communicate with people about giving.
    No if its gift aid, it is derogated (allowed). Yes if it's general giving or fundraising.
33. Will Church House Publishing or SPCK be updating their standard forms for baptism applications and wedding banns to include consent for the Church to inform them about upcoming consents?
    This is pending. Assume that they will but in the meantime please make your own arrangements to gather any necessary consent, i.e. if you plan to send families information on events and activities following the baptism.
34. What is the position about weddings / baptisms / funerals from past years? I guess we can send baptism anniversary cards and Christmas cards to wedding couples provided it is simply that, if we use it to advertise or fund raise then presumably we will need consent?

You do not need consent to send anniversary cards, assuming the recipient is someone you are in "regular contact" with. Regular contact does not mean frequent, so this would be fine even if the recipient only attended the Easter service every other year, for example. Anniversary cards are great, and you might also want to add in the card the website of the Church, or just an encouraging sentence that you hope they might like to look at the Church and what it's up to. We assume that the cards would be sent in the post, the rules are a bit more restrictive for email communications and for email you will often need to get consent. This is because the card may count as marketing (especially if you do decide to include some wording encouraging them to look at what the Church is up to) and email marketing almost always requires consent.

35. I have contact details for family members which I have obtained through funerals, weddings, baptisms and so on. Do I need consent before I contact them about events? Also, do I need consent before sharing their contact details with other vicars?

    There are a number of points to consider here. First, you need to make sure that individuals know that you have got their details and why. As part of this, they should be provided with a copy of the privacy notice. Whether you can contact them without consent will depend on the reason why you want to contact them. For example, if it is to invite them to attend a fundraising event then we suggest that consent should be sought. You will need their consent before sharing with other vicars unless that sharing was clearly within the expectation of the individual concerned. For example, you would not need consent if a vicar had to step in to cover a funeral at short notice.

36. Currently, material is frequently sent home with children promoting events at church that have nothing to do with school life. Do our schools now have to obtain the express permission of parents to communicate with them about church rather than school affairs? The Diocesan vision wishes us to consider our schools as an extension of our worshipping communities but these regulations appear to work in precisely the opposite direction.

    The "belt and braces" approach would be to seek consent. However, there is a strong argument that seeking consent is not necessary but there is a risk that this could be challenged by the ICO (the data protection regulator). If you decide not to seek consent then the School should still notify parents and pupils about the practice. This gives parents (and older pupils) the opportunity to object. Where parents (or older pupils) do object, the School should keep a list of these to ensure that material is not sent home with these particular children. The church material should be passed to the School to distribute to the children. The School should not pass on personal data to the wider church without consent (even if it decides not to seek consent for the initial communication to parents). If the parent wanted to attend a church event, they should either contact the relevant parish direct or give their consent to the School passing on the information.

37. Can parents give consent on behalf of their children for GDPR purposes?

    Children can exercise their own rights in relation to their data once they are mature enough, which in practice is often taken to be from and including the age of 12. This means that any consent should often come from the child (rather than a parent) once the child is aged 12. However, in many cases it will still be appropriate to involve the parent until the child is older, eg, by requiring both the parent and the child to sign the consent form until the child is 16. For children who do not have sufficient maturity (ie, the majority of those aged 11 and younger) the

parent can give consent on behalf of their child. If you are offering an online service to a child and you are relying on consent as the basis for doing this then the consent can come from the child once the child is aged 13. In other words, the general rule that children can exercise their rights from and including the age of 12 is displaced for online services where consent is sought.

38. We often send out named invitations to the whole village to attend special services. Can we do this without specific permission?
    You will need specific permission for this.
39. Can the Church discuss in person with parishioners who are not necessarily regular church attenders about the Parish Giving scheme?
    You can always have a conversation and hand out any information fact sheets etc that people can then take further if they wish. It would also be fine to publish something on the parish website or parish Facebook wall, for example.
40. When do we not need consent to process special categories of personal data (such as information about religion)?
    Under the GDPR, religious (amongst others) not-for-profit bodies may process data without specific consent as long as it is for legitimate purposes and relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent. We are calling this the "legitimate purposes" rule. As an exception consent will still be required for certain types of marketing communication even if the legitimate purposes rule applies. For example, you will still need consent to send a fundraising email.
41. What does "consent" really mean in practice? Does it have to be in writing? Also, can consent be implied (for example, we have been sending parishioners newsletters for years, can we treat it as valid consent if they have never opted-out or complained)?
    Under the GDPR, consent must be freely given, specific, informed and unambiguous. In many cases, it will need to be explicit as well. This means that the following should be kept in mind in particular: (1) Consent should be sought using a form which requires the individual to tick a box to consent (opt-in consent). If the form states that the individual will be treated as having consented unless they state otherwise then this will not count as valid GDPR consent. (2) You should break down the consent as much as reasonably practicable. For example, if you are seeking consent for two different things then you should have a separate tickbox for each. In addition, if you are asking for consent to add a parishioner to your mailing list then you should have a separate tick box for each channel of communication, for example: email, post, text message. (3) You must not "bundle" consent with other matters. For example, imagine a parishioner was told that appearing on the electoral roll meant that they were deemed to consent to receiving the parish newsletter. This does not count as valid consent. (4) People must be told about their right to withdraw their consent and it must be as easy for someone to withdraw their consent as it is for them to give it. (5) You must keep a record of consents obtained.
42. We send a Benefice Magazine to every household in the benefice which advertises Benefice Church events and also has advertisements from local or relevant traders. Should we be getting consent to deliver this before we push them through people's letterboxes?
    You only need consent if you are processing personal data in relation to sending out the magazine. For example, if the magazine is being sent to every household in the

benefice and is addressed “Dear Resident” rather than “Dear Mrs Smith” then consent is not required.

43. Do we need consent before sharing information about people who help out in the Parish? For example, we give flowers to comfort people (eg, if they are bereaved) every Sunday. We have a rota so that volunteers know when they are on duty. Do we need to get consent from a volunteer to share the rota with other volunteers?
    This does not require consent so long as the rota is only shared with clergy, staff and volunteers. If the rota was to be made available to the public (eg, if it was printed on the noticeboard in the church) then consent would be required. Please note that consent must be specific, so if someone had consented to appearing in the directory you would need another consent for the noticeboard.
44. Do we need to get all of our existing consents with people renewed?
    Not necessarily. Where you rely on consent, the ICO has stated that it will not be required to obtain fresh consent from individuals if the standard of that consent meets the requirements of the GDPR, i.e. consent has been clearly and unambiguously given and you have a record of that consent.

    Nevertheless, it is important to review all consent mechanisms to ensure that they meet the standards required under the GDPR. If you cannot reach the high standard of consent as set out in the GDPR, you must look for an alternative legal basis for processing the data or stop processing the data in question. Under the GDPR, consent must be verifiable. This means that some form of record must be kept of how and when consent was given. Consent must be freely given, specific, informed and unambiguous (i.e. consent requires clear affirmative action from an individual (i.e. the data subject)). Silence, pre-ticked boxes or inactivity (e.g. just staying on a website or not responding to a request) will not be sufficient. Individuals must also be informed of their right to withdraw consent at any time and how they can do this. In fact, it should be no more difficult to withdraw consent as it is to grant it.

Security

45. Is the home computer secure enough - are we falling foul of any rules?
    Is it secure? What measures have been taken? It should have a good antivirus, passwords that only the relevant user knows (i.e. other members of the family should not be able to access the information). Is it on a laptop that could accidentally be left on a train? Is it possible to encrypt it? How are you sending it to others (email, paper)? You need to consider what data is held and how easy it would be for another to access it and decide if you need to act on this.
46. Is it ok for me to use an online document storage system, for example Google Drive or Dropbox?
    In principle yes, but you need to make sure that it is used in a way that is data protection compliant. In particular, you should carry out a data protection impact assessment, which will involve thinking about: (1) What you plan to do; (2) An assessment of necessity and proportionality; (3) What the risks are; and (4) How to mitigate those risks. One of the features of many online document storage systems is that they are designed to make it as easy as possible to share information. As such it is important to make sure that the system is going to be secure in practice. The sorts of questions you may wish to ask include Is there a risk that documents could be downloaded to someone’s personal computer? Could access

permissions be changed inadvertently? Some organisations have concluded that using "off the shelf" document storage systems is too risky and instead use bespoke systems. This may be especially relevant to where the platform is intended to be used to store information which is especially sensitive, such as safeguarding or child protection information. It is possible to purchase software which is specifically aimed at protecting high risk information, such as child protection information.

47. I understand that under data protection law we need to make sure that the personal data we have is kept secure. This is not something I have thought about before. Where do I start with this?
    The starting point is that you must make sure that you have taken appropriate "technical" and "organisational" measures. Technical measures cover things such as using encryption, making sure that data is backed-up and so on. Organisational measures concern training staff, clergy and volunteers on the data protection risks, having written data protection policies and procedures in place and auditing your data protection compliance. It is important to think about how you can apply these principles in practice. For example, when people work "on the go" or use a family computer for PCC and / or parish matters.
48. I need to enter a password before I can access the start screen on my laptop. Does this count as encryption?
    Encrypting data means that the data is encoded such that it cannot be accessed without knowing the key to unlock it. Sometimes the key is in the form of a password that must be entered before the data can be read, but there are other types of encryption. For example, sometimes data can only be unencrypted after you have inserted a key fob into your computer. The password you enter when you first turn on your laptop does not count as valid encryption.
49. We have lost a laptop containing staff and payroll information. The laptop also contained scanned copies of staff employment contracts. The laptop was not encrypted. Do we need to tell anyone?
    You must inform the ICO (the data protection regulator) within 72 hours of becoming aware of the incident unless the incident is unlikely to put individuals at risk. In addition you must inform data subjects themselves if the risk is "high". In this case, owing to the possibility of identity theft, it is likely that the ICO and staff will need to be told. In addition, you will need to inform your insurers and you may also want to report this to the Police.
50. I have heard a lot in the news about cyber threats and organisations being hacked. Is this relevant to our parish?
    If you have been hacked as a consequence of failing to put adequate measures in place to protect your systems then you will likely be in breach of the GDPR (assuming personal data has been put at risk). There are a number of online resources to help deal with cyber threats. This includes Cyber Essentials, which is a government backed scheme containing standards relevant to cyber security. Further information can be found here: https://www.cyberessentials.ncsc.gov.uk/
51. Can our volunteers use personal email addresses?
    The Information Commissioners Office (ICO) have said that it is not good practice to use personal or work email addresses to work on sensitive information on the church's behalf. This is because the email provider will have no official relationship with the church (as a Data Processor would) and have no vested interest in the church as a Data Controller.

Using a work email address would potentially involve the employer in a negative situation if there was a data breach and could have implications for the employee. It would also suggest that the volunteer's church business was on behalf of their employer.

Another issue facing lots of churches is how to document and monitor the information which is held by volunteers outside of church offices or online services. Again, we recommend (based on the ICO's advice) that you do not allow data outside of church control. At the very least you should work towards this by having a written policy documenting who has access, where the data is kept, how long it is kept for, and in what format.

This does not mean that you cannot communicate with Data Subjects using their own personal addresses, but that you should use official church email addresses to do so.

52. What do I do about the email addresses that my email system remembers and autocompletes?
    Autocomplete email addresses would fall under the description of personal data for the purpose of GDPR if they contain a name such as bob.smith@ but would not if they were info@. Unfortunately there is not a clear yes or no answer. You can rely on legitimate interest in keeping these as they are added when you reply to an email. It would be safe to say that if you stop contacting someone they would get removed from the list, please take a look at https://support.microsoft.com/en-gb/help/2199226 for and explanation from Microsoft as to who the process works and how you can remove them.

    There are safeguards for Outlook if you are using cloud based software and you would still require passwords to control access to the emails. If you have a physical server you would need to ensure that it is secured with passwords, anti-virus, a firewall and so on.

Sharing data

53. How can we continue to provide good, team-based pastoral care in these circumstances, especially where different members of the team may visit/receive updates, and where visits are less frequent (and therefore especially important to have written 'memories' of what happened/was discussed/etc on the previous visit)?
    The priority is keeping the data safe. Sharing it only with those who need it – i.e. the team; locking it away and having a system for making sure it is as up to date as possible.
54. Can we put up a list of our electoral roll members or the Parish officers, including their contact details, on our notice boards?
    Yes
55. A local charity has contacted us because they are looking for volunteers. We think that a number of our own volunteers would be a good fit for the charity. Can we pass on their details to the charity?
    Not without consent.
56. Once people have agreed to be in the directory/congregation list, which we currently only give to people in the directory/ congregation list, with say 200

copies distributed it is virtually impossible to ensure that it won't be shared, even if you print on the directory that the information in it may not be shared with anyone not included.
You need to make sure that the consent form makes it clear that the directory will likely be shared with the public at large.

57. Can we still send details of deanery synod elections and churchwardens elected etc. to the diocesan office. Will we need consent to do this?
Yes you can share this information with the diocese – managing and administering the elections will require the dioceses to process this information, this is stipulated in the Church Representation Rules. Consent will not be needed for the data to be shared for this purpose. Indeed, if you stand for election you would expect your data to be shared with the diocesan office. The Rules state that the results will be sent to the Diocesan Electoral Registration Officer.
58. My parish is in a multi-parish benefice – how do the consent and privacy forms relate to that situation rather than the single parish/benefice situation?
Provided you make it clear in your privacy notice and consent form that you are processing the data on behalf of the whole organisation – whether a single or a multi-benefice organisation then it will be ok to use a single privacy notice and consent form.
59. We have paid staff and the payroll is provided by another organisation (e.g. a diocese or payroll service provider) – can we still share information with them?
Yes – The 3rd party is processing data on your behalf. You do though need to make sure that the contract you have with them is compliant with the GDPR (speak to your diocesan registrar and/or data protection officer at the diocesan office), in particular it will need to set out in clear terms what the organisation is doing with the data on your behalf and its location and security.

General

60. Do I need to register us with the Information Commissioners Office (ICO)?
Under current rules, most organisations that act as a Data Controller need to register with the ICO and pay a notification fee of £35 or £500 (depending on the organisation's size) unless they are exempt.

Some churches may be exempt if they process only the following data:

- Church membership list (where church members have provided their own details)
- Gift Aid information
- Payroll and Accounting records

If you gather or store any personal data which is not on this very limited list, you should be registered with the ICO. This includes any pastoral notes and any communications to or from church members which mention personal information, as well as any fundraising requests. In real terms, very few churches will find themselves exempt.

It is also important to note that exemption from registration and the fee does not mean exemption from complying with Data Protection Legislation. You are still expected to comply with the current legislation and that will not change under GDPR.

If you are not sure whether or not you should currently be registered, you can use the ICO's own self-assessment tool: https://ico.org.uk/registration/new

61. What is a privacy notice?
    A privacy notice (also known as a transparency notice) is to inform parishioners (and other individuals that you hold information about) how their personal data is used. Providing a privacy notice is part of the obligation to process personal data fairly, which is a fundamental principle of data protection compliance. You can find a sample privacy notice here: http://www.parishresources.org.uk/gdpr/
62. How do I go about providing a privacy notice?
    A copy of the privacy notice must be provided to the individual when they first provide their personal data. If the individual's personal data is provided by a third party then the privacy notice must be provided to the individual on the earlier of: a reasonable time period (being no more than one month); when you first communicate with the individual; and if disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed to that recipient. The notice should also be published on the parish's website (in addition to being provided on request) so that it can be easily accessed for future reference There should be a link to the privacy notice on every page of the website. It goes without saying that providing the privacy notice should be done with the appropriate level of sensitivity. For example, if you are discussing funeral arrangements with a deceased's relatives then it may not be appropriate to hand them a lengthy privacy notice at the first meeting. An alternative might be to include a brief summary of key information (eg, in a FAQ document covering other matters relating to funeral arrangements) with a link to the full version of the notice on your website.
63. Who do I need to provide a privacy notice to?
    A privacy notice should be provided to anyone about whom the parish will hold or process personal data. This includes children, as well as adults. Children are permitted to exercise their own rights in relation to their data once they are mature enough which is often taken to be from and including the age of 12. Therefore, we would recommend providing an age-appropriate privacy notice to children once they reach this age
64. How do I recognise a subject access request?
    An individual has a right to request a copy of the personal data held about them. This is known as making a subject access request or SAR. A SAR does not have to be labelled as such and does not even have to mention data protection. The only requirement is that the request is made in writing, verbal requests are not valid. For example, an email from a parishioner or clergy person which simply states "Please send me copies of all emails you hold about me" is a valid SAR.
65. When do I need to carry out a data protection impact assessment?
    Under the GDPR organisations must carry out a data protection impact assessment (DPIA) if what is planned is likely to result in a "high risk" to individuals. The following are all examples of when it would be appropriate to carry out a DPIA: If you plan to introduce a new IT system or use or store personal data in a different way (for example, if you decided to switch from paper to using online storage such as Dropbox). You should also carry out a DPIA before carrying out monitoring (eg, CCTV or installing software to track staff internet browsing habits). It is also good practice to carry out a DPIA in relation to any personal data you hold about children. The DPIA must include 1. A detailed description of what you plan to do

and why (including legitimate interests relied on); 2. An assessment of necessity and proportionality (ie, "is what we are doing necessary and proportionate"); 3. An assessment of the risks; and 4. Steps taken to mitigate those risks.

66. Do we need to complete a data audit? Yes, and there is a simple template on the Parish Resources website to help you do this: http://www.parishresources.org.uk/gdpr/dataaudit/
67. I would like to collect information about parishioners even though I am not yet sure what I want to do with that information. For example, we are thinking about new events and activities to improve engagement but we don't have any fixed plans yet. What do we need to do?
    First, you should make sure that what you are planning to do is covered by your privacy notice. In some cases you will need consent before you collect information. However, you cannot be collecting personal data on the off-chance you might need it for some future (as yet undefined) purpose. Therefore we suggest that you hold off for now until you are clearer about what you plan to do.
68. What do I need to do to make sure that the information we have is accurate?
    You must take "every reasonable step" to ensure that the personal data you hold is accurate. For example, staff and volunteers should be reminded on an annual basis to tell you if their details have changed.
69. Should I report a data breach and when should I do it?

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify.