DIOCESE OF SODOR AND MAN

FAQs February 2019

Who is the data controller for parish information?	The PCC, the Church Wardens and the incumbent are separate data controllers.
Who is the data controller for Diocese information? Who is responsible for compliance in the Diocese?	The Diocese of Sodor and Man is the Data Controller. It has nominated key individuals to the Diocesan Data Protection Group to ensure adherence and compliance. In the first instance we would ask you to raise any queries/ concerns/ complaints to the Bishop's Chaplain, The Reverend Ben Bradshaw, phone: + 44 1624 622108 chaplain@sodorandman.im
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.
Who will be the data controller for data that the "incumbent or priest-in-charge" holds?	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.
Is the phrase "incumbent or priest-in-charge", when used in the parish resource leaflet, 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 the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations .	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.

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.
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.
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.
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. 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?

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. The rules are more restrictive for email communications than postal 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.
Is consent required to send invites to an 'All Souls Service' for past funerals?	You do not need consent to contact people about the All Souls Service if the individual is someone you are in regular contact with. However, where there is no regular contact (which may often be the case for family members of the deceased) we suggest that the best way round this is to ask them verbally if you can stay in touch and if they say yes send a follow up card/letter along with a consent form and envelope where you can specifically let them know how you'd like to be in touch with them, include in the letter the details of the service and how their loved ones' names will be remembered/read out, and they can then sign their consent for you to be in touch (and your consent can be for five years – and they can withdraw at any stage eg if they move away). The actual anniversary of death or funeral is a matter of public record so these can be stated in a parish magazine. In addition, the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations only applies to living individuals.
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. 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.
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 they do object, the School should keep a list of these to ensure that material is not sent home. The church material should be passed to the School to distribute to the children. The School should not pass on personal data 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.
We often send out named invitations to the whole village to attend special	You will need specific permission for this.

services. Can we do this without specific permission?	
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 confidentially shredded. 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.
When do we not need consent to process special categories of personal data (such as information about religion)?	Under the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations, 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.
Can parents give consent on behalf of their children for the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations 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.
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.
I understand that under data protection law we need to make sure that the personal data we have is kept secure.	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

This is not something I have thought about before. Where do I start with this?	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.
What is encryption?	Encryption is a mathematical function that encodes data in such a way that only authorised users can access it. It is a way of safeguarding against unauthorised or unlawful processing of personal data and is one way in which you can demonstrate compliance with the security principle. Encryption protects information stored on mobile and static devices and in transmission, and there are a number of different encryption options available.
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.
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.
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 Information Commissioner (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 IC 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.
We send a church magazine to every household in the parish which advertises church events and also has advertisements from local or relevant traders. Should we be getting consent to deliver this before we push them through peoples 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.
Under the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations individuals have a "right to be forgotten", ie a right to have their personal data deleted. We have some historic information relevant to an allegation	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

made against a former clergy person. Can that individual exercise their right to be forgotten and require us to delete their personal data?	interest, this will likely apply in many cases where historical allegations have been made.
Our staff and volunteers use their personal laptops for parish matters. Is this compliant?	This is a tricky area because the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations requires you to go to great lengths to protect information held on computer (and paper records as well). Allowing staff and volunteers to use their personal laptops without any extra protection in place is unlikely to be compliant. You could think about giving staff and volunteers secure remote desktop so that everything they do is saved centrally to the parish systems, but we do appreciate that this is not practicable for many parishes. An alternative, which will go a long way to reducing the risks (even if this is not quite enough on its own for the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations purposes) would be to require staff and volunteers to encrypt anything on their computer that is church related. Some modern computers come pre-installed with encryption (which means that the data is encrypted automatically without staff / volunteers having to do anything) and it is also easy to download encryption software from the internet. In addition, you should ensure that staff and volunteers are given training on the data protection "dos and don'ts" and that this training is backed up by written policies and procedures.
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.
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.
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.
Is it OK to use memory sticks (also known as USB sticks) to store personal data?	This should be avoided if possible. Memory sticks are easily lost, it would be better to store personal data centrally. If memory sticks are to be used then at the very least we suggest that they should be encrypted.
Can we keep personal data for historical research purposes without consent?	The short answer is yes although the General Data Protection Regulations and Law Enforcement Directive Implementing

	Regulations 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.
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.
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.
Will we need to seek consent to publish the electoral roll?	No – As the Church Act 1987 requires publication, then this is a legitimate activity of a not-for-profit body under the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations and so data can be processed in this way. In addition, by applying to have their name placed on the electoral roll individuals are consenting to their personal data being processed in accordance with the Church Act.
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 CRR. 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.
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.
Children and the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations	With regard to children, the ICO has stated that if an organisation offers services over the internet directly to children (in the UK, under the draft Data Protection Bill, this will be anyone under the age of 13), then you will need parental consent in order to process their personal data lawfully. Other than this, there is little fundamental change to the rights

	of children, who are considered as individuals in the own right. Children's data, (where on-line services are not involved) is covered by the fact that children are considered to be a vulnerable group and therefore warrant specific consideration and protection (i.e. they must be provided with clear information about what, why, how etc, and must be able to understand the risks, consequences and safeguards and their rights), but otherwise are accorded the same protections as adults in the DPA and the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations. Specifically: a. You must have clear and age-appropriate privacy notices for children. b. The right to request erasure is particularly relevant when consent was given when the individual was a child. c. The concept of competence remains valid under the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations – you may wish to give an individual with parental responsibility for a young child the ability to assert that child's data protection rights on their behalf or consent to processing their data. d. If an older child is not deemed competent to consent or exercise their own rights you may allow an adult to do this. e. You can still process a child's data under legitimate interests. f. Privacy by design is the same and should be properly considered when processing children's data. g. So for example with regard to a youth group mailing list – parental consent may be considered appropriate depending on age and competence i.e. do the children understand the implications of the collection and processing? If yes, they can give their own consent unless it is clear they are acting against their own interests.
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 General Data Protection Regulations and Law Enforcement Directive Implementing Regulations (speak to your diocesan registrar and/or data protection controller 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.
Do we need to get all of our existing consents with people renewed?	Not necessarily. Where you rely on consent, the IC 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 General Data Protection Regulations and Law Enforcement Directive Implementing Regulations, i.e. consent has been clearly & unambiguously given & 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 General Data Protection Regulations and Law Enforcement Directive Implementing

	Regulations. If you cannot reach the high standard of consent as set out in the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations, you must look for an alternative legal basis for processing the data or stop processing the data in question. Under the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations, 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 -the data subject). Silence, pre-ticked boxes or inactivity (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 & how they can do this. In fact, it should be no more difficult to withdraw consent as it is to grant it.
What are the implications of the incumbent being a separate date controller?	The incumbent is responsible for ensuring that they manage personal data provided by data subjects in line with the General Data Protection Regulations and Law Enforcement Directive Implementing Regulations, so all of the guidance provided is applicable to incumbents as well as PCCs.
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 General Data Protection Regulations and Law Enforcement Directive Implementing Regulations 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 General Data Protection Regulations and Law Enforcement Directive Implementing Regulations 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.