# Initial data protection advice for churches and circuits (GDPR)

I think it is fair to say that in our desire to be open and obliging, we Methodists – paid and volunteer – have not been as careful with people’s information as we should have been. Although this new legislation might seem like a bureaucratic burden, we should perhaps view it as another means by which we can show our care for our people. It is important to respect people’s privacy and show that we recognise the trust that is placed in us by those who hand over their personal information. Most of the responsibilities enshrined in the new law are already on the statute book, and we have, perhaps, not taken those responsibilities as seriously as we should have. So…this is a great opportunity to up our game!

## Although the legislation comes into effect on 25 May, it is recognised that most organisations will not have everything in place by that date. The important point is that you can show that you aware of your responsibilities and taking steps to meet them.

I have tried to think of real situations where we might come unstuck as examples. If you have any queries, you can start by asking me and I will try to find the answer for you.

## Guiding principles

* Don’t keep information that you don’t need or are not entitled to
* Keep information securely and don’t allow others to access information that they don’t need
* Tell people that you hold information about them and why

## Don’t keep information that you don’t need

* You need a good reason to hold information about individuals and you need to be clear what that reason is.
* The new regulations provide several reasons – ‘lawful bases’ – but only two will have much relevance to churches; **legitimate interest** and **consent**.
* **Legitimate interest** entitles you to keep information that you need to conduct your ‘business’. For example, you are entitled to keep contact information about church members, financial details of people giving by standing order, or details of regular hirers of church premises. Providing the data you hold is necessary for the job you are doing, only used for that purpose, and that people would reasonably expect you to have this information about them, then you do not need consent. But the principles of ‘need’ and ‘purpose’ are important. You *need* to know where your church members live; you *do not need* to know who else lives in their house. You might want to have that information for pastoral reasons, but it is not necessary, and therefore you would need to get the consent of the non-church members to keep information about them. Similarly, you can legitimately store the email address of a local plumber for the purpose of asking them to work on the building; you cannot use that email address to invite them to a church event as that is not the purpose for which the information was provided. One area to watch out for is contact with people outside the church whose information you have received for specific purposes, for example, couples wishing to marry in the church or families of those whose funerals have been held in church. You cannot contact those people after the event, without their permission. It would obviously be inappropriate to present people with a consent form at the baptism, wedding or whatever, but you could always ask them if it would be ok to stay in touch and then follow up with a card and consent form. Although we might want to argue that our purpose, as we interpret it, is to evangelise the member’s husband or the plumber, or provide support to newly-weds or recently bereaved, this would not be considered the core business of the organisation for data protection purposes and would not constitute a legitimate interest.
* **Consent** will be necessary for information that is not covered by the legitimate interest lawful basis. The main area where this will apply to us is in published information. Because printed directories, plans etc cannot be prevented from being accessed by third parties then consent will be required for the information that is printed in them. In other words, we are choosing to make the information available to people who do not need it – who do not have a *legitimate interest*. Once it is printed and, for example, pinned to a church notice board, then it is in the public domain and consent will be needed.
* Where consent is given, it must be **recorded**. If you use a consent form, then keep those forms either in hard copy or electronically. In some circumstances, verbal consent would be sufficient, but it must still be recorded with the date, reason, and to whom it was given. It will be worth setting up a spreadsheet/database to keep track of consents.
* **Children** 13 and over are expected to provide their own consent, where consent is required. Parents/carers can only consent on behalf of teenagers where it can be shown that the young person is not able to give their own consent.
* You will not need consent for **newsletter circulation** except in particular circumstances. If your mailing list is very old, or you’re not sure how you came by the addresses, it might be an idea to seek consent. The situation where consent is essential, is for direct marketing. The ICO is clearly defining direct marketing as including any requests for money, including church fundraising. So if you ever include information on fundraising **with an invitation to contribute** then that would be considered direct marketing and you will need informed consent from everyone that you contact. You can advertise the quiz evening to raise funds for the church roof in your newsletter without consent, you cannot write that the church roof is in need of repair and contributions would be welcome without consent. Subtle difference, but important. (There is an argument that all church activity advertising is direct marketing, but that doesn’t seem to be the current position of the ICO. You could future-proof your lists in case they change their mind by including a tick box for direct marketing – with an explanation – on your consent form)
* Now would be a good time to conduct a **data audit** – a thorough look at all the information held by your church/circuit and whether it is all necessary and up-to-date. Part of the obligation in managing data is not to keep it longer than is necessary, so information on people who have held roles in the past, old directories and plans, obsolete rotas should be destroyed (with perhaps one copy held securely for archive purposes in some cases). The less information you hold and publish, the less vulnerable you are to data breaches. You should also have a policy for retrieving information held be people who then leave their post (stewards, children’s workers etc). Everyone who holds information should be advised on how to dispose of it – thorough deletion of electronic records, shredding of paper records.
* Consider having different levels of access to information. Not everything held by your church or circuit secretary/administrator needs to be accessible to everybody all the time. Someone might need to know who sits on a particular committee, or the address of an elderly member, but they probably do not need to have constant and open access to that information. It is not unreasonable to expect someone to ask for rarely needed information rather than to have everything at their fingertips. Consider advertising *where to find* information rather than the information itself.

Keep information securely and don’t allow others to access information that they don’t need

* Having established what information you hold, and the lawful basis under which you do so, you have an obligation to manage and process that data securely
* Any data held electronically (laptop/tablet/desktop/smartphone) must be protected, by the file, folder or device itself being password protected or encrypted. The standard password-to-log-on with Windows will not be sufficient.
* Data should not be available to anyone who doesn’t need it, so probably best not to pin rotas with contact details to church noticeboards – even names count as data so get consent for your church welcomers list or flower rota to be on display in the vestibule.
* Great care should be taken in emailing as this is the easiest way for information to fall into inappropriate hands. Where contact information for a group is held, it should ideally be managed by one person rather than a spreadsheet of addresses being circulated among the whole group. Where there are rotas to be managed, perhaps only the organiser needs all the details. If a group of people need to contact each other to arrange meetings/duty swaps or whatever, ensure that they have given their permission for that information to be shared (and that that permission is recorded).
* When sending group emails then the BCC (blind copy) option should always be used to prevent mass circulation of email addresses. This does have the downside that email recipients don’t know who else has received the information, but this can be overcome by putting a line at the head of the email saying ‘This email has been sent to all church members/pastoral visitors…’ or whatever.
* Be very wary of family/couple email addresses. Where people share email addresses such as johnandsue@hotmail.com or thesmiths@gmail.com there can be no expectation that information is being received only by the appropriate person. Knowingly using shared email addresses could be considered a data breach.
* Watch out for autocompletion of email addresses. I receive emails each month that are intended for circuit administrators. This is because the sender has begun typing ‘admin..’ into the email address bar and the autocomplete system has wrongly predicted the address and defaulted to another similar email address. Each time this happens in the future will be a data breach that should be recorded.
* If you have someone on an email list that never seems to reply, it will be worth checking that you have the correct address. We recently heard from a gentleman in Dallas, Texas who has been receiving local preacher information from us for years. His email address is one letter different from someone in the district.
* Personal information held in paper form should be secure. This could be in a locked filing cabinet, or in a room that is only accessed by those entitled to use the data. Ministers need to be careful of storing information where other family members could access it.

## Tell people that you hold information about them and why

* This is where the all-important **privacy notice** comes in
* Whenever you collect or display information, you must have a privacy notice. This tells people why you are asking for their information, what you intend to do with it, who will be able to access it, how you will store it and for how long, and a contact process for queries. A model privacy notice is being prepared Connexionally but you can devise your own if you follow these guidelines, as the notice is likely to vary in different contexts.
* Websites must have the notice and any data collection/consent forms should have this information very explicitly. All information should be opt in – it will not be enough to say ‘unless I hear from you, I will assume that you are ok with receiving the newsletter/appearing on the plan etc’
* If you have CCTV cameras on your premises, this needs to be referenced in your privacy notice, as images count as personal data.
* You can see the Methodist Church’s privacy notice on its website at <http://www.methodist.org.uk/privacy-and-cookie-policy/>. You probably won’t need anything quite so comprehensive. The ICO has produced some examples of dos and don’ts here <https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf>
* Individuals have a right to have their data erased – this is known as the ‘right to be forgotten’. It is not an absolute right – you cannot request that the tax office expunge all information about you – and safety concerns trump data rights. Where data held relates to safeguarding concerns then there is unlikely to be a right to erasure. For any data issues relating to safeguarding, please contact the District Safeguarding Officer for advice.
* Individuals have a right to correct false data – this could be an issue for directories etc. When an individual notifies you that their email address has changed, it will be your responsibility to send that correction to *everyone that you have circulated that information to.* You could probably put a timescale for that in your privacy notice, for example, stating that an update will be issued half way through the year, but it remains an obligation that could become quite onerous and is another argument for limiting published data as much as possible.

## Special category data

## This refers to information that goes beyond basic contact details, date of birth etc. It includes information relating to ethnicity, health, political opinions, sexual orientation, sexual relationships, criminal convictions, and **religion.**

* Because almost all of the information we hold would identify a person’s religious affiliation, we become subject to stringent rules *when that information enters the public domain*.
* We might initially think that we do not operate in the public domain, with the exception of directories and plans, but many churches and circuits have a **Facebook, Twitter or Instagram** presence and a website. If you post a photograph of a service or church event in which people are identifiable, then you are processing their special category data and you must have their **consent.** This would not apply to individuals, only organisations, but if you allow individuals to post on your church Facebook page then their posts might be your responsibility (I am trying to get a definitive answer on this). While Church House is thinking about this, consider putting a notice at the top of your page asking people not to post photographs of identifiable individuals without having their recorded consent.
* Consent can be verbal in these situations – a minister might announce that he is taking a photo of people around the Easter floral cross with the intention of posting it on Facebook and suggest that anyone who does not want to be included should step away – but he or she would need to record that consent was obtained.
* This would also apply to **videos and live streaming**. It is not practicable to get informed consent from an entire congregation so consider videoing only those presenting, or a small section of the congregation/audience who have given their consent.
* Please make sure that the option to withhold permission is a real one and people do not feel pressured to comply.
* Take special care with **pastoral information**. Any notes relating to health (including mental wellbeing), vulnerabilities or relationship issues, for example, would be regarded as special category data and the utmost care should be taken to ensure that this data is stored securely and is only shared as necessary.

## Other points to note

* Look carefully at **registration forms** for Messy Church, holiday clubs etc – only request the information you actually need. Where parents/carers are in attendance then very little information is necessary. Where children are left in the care of church workers, then more might be needed – health information, emergency contact. In most cases, home addresses and dates of birth are unnecessary. Be careful with photographs. And remember the privacy statement.
* **Data breaches** must be logged, and in some cases, reported to the ICO (Information Commissioner’s Office). You must keep a record of any mistakes, which could be anything from having your laptop stolen to emailing the wrong person by mistake with information about someone else. Sharing email addresses without permission would also constitute a breach, so remember the BCC function.
* The Methodist Church is responsible for the data management of all Methodist activity, so expect **policies** to be produced that we will all have to sign up to in the near future.

## Some terms and titles

* Data Controller – the person/entity responsible for data management in your organisation; this is the Connexional Methodist Church for all our local activities
* Data Processor – anyone who handles personal information
* Data subjects – any living person that we hold information on
* Personal data – any information that relates to an identifiable living person
* Data Officer – do not appoint a Data Protection Officer; this is a professional role with statutory obligations.
* Data manager/champion/administrator – suggested titles for anyone appointed locally to oversee compliance
* GDPR – General Data Protection Regulation. Passed by the European Parliament in April 2016 and will become enshrined in UK law in May this year (so still in effect post-Brexit!)
* ICO – Information Commissioner’s Office. A public body, reporting directly to parliament, which has oversight of GDPR compliance.