St. John's Wimborne
New Life, Full Life

GDPR Briefing
St John's Church, Wimborne

What is GDPR and what does it mean for churches?

GDPR stands for the General Data Protection Regulations and is the largest shake-up in data protection law in over 30 years. GDPR came into effect on 25th May 2018. It is EU legislation but irrespective of Brexit the UK Data Protection Act 2017-2019 will integrate all its effect into UK law.

Some basic jargon explained…

DATA CONTROLLER
As a church we are a **DATA CONTROLLER.** This is our role. We gather data. We store it and we process it. Our responsibility is to make sure that we do this in an appropriate, respectful, transparent and honest way and in line with the stipulations in the GDPR legislation.

DATA
For the purposes of GDPR, **DATA** is anything that can identify an individual. This often means; names, email addresses and contact details, dates of birth and other family information. Obviously as a church we will often need to hold this information but we mustn't think of this DATA as our own. We are stewards of it, but it remains the individual's data. It is a digital representation of someone, and that person has the right under GDPR to know it exists, know how we're using it, where we're storing it, for how long and how they can have it back (**RIGHT TO BE FORGOTTEN).**

DATA PROCESSOR
If we use a piece of software or CMS (such as ChurchSuite, Data Developments etc.) to store our data, or a gift aid or accountancy package, those companies are our **DATA PROCESSOR**. We need to ensure that we only work with data processors who are GDPR compliant. NB ChurchSuite and Data Developments are compliant!

DATA ASSET
We have lots of **DATA ASSETS**. Every list, spreadsheet, register, collection of forms, address book etc. is a separate data asset. As part of our compliance with GDPR we should maintain an up-to-date catalogue of all our data assets, assign a responsible person for each asset (an Information Asset Owner IAO), list it in our privacy policy and have a routine of review, data purging and retention for each asset. Therefore, a good 'house-keeping' task is to reduce the number of data assets we have and operate with as few as possible which still effectively facilitates our ministry. The use of ChurchSuite will help in this regard as it is several modules using the one database.

MANDATORY NOTIFICATION OF BREACH
A significant change under the introduction of GDPR is our **MANDATORY REQUIREMENT TO NOTIFY DATA BREACHES** to the ICO (Information Commissioner's Office). This means from 25th May onwards, if we become aware that a list containing personal data goes missing, an unencrypted and un-password protected laptop is lost (or left on a train) or an email containing personal data is incorrectly sent to an unauthorised recipient outside your organisation, you have a legal obligation to report this as a data breach within 72 hours. Therefore, taking steps to reduce

this risk, and implementing appropriate I.T. security and use of passwords is sensible and prudent. Fines for data breaches can be extremely large depending on the nature & size of the breach.

CONSENT

It's important to consider 'how' we have obtained data, 'why' we have it and 'what' the owner of that data permits us to do with it. **CONSENT**, is one aspect of GDPR and provides a mechanism, permission and an audit trail for why we are using data in a certain way. (It is not always required and I'll come on to this later), but having consent will prove helpful in many situations and contexts. Consent should always be clear (clearly explained and easy to understand), specific (for a particular purpose), freely given (always an opt-in, not opt-out and not a requirement), transparent and demonstrable. If we've gained consent from an individual, we need to be able to evidence this. The problem with solely going for consent is that many people don't get around to replying and giving their consent and many organisations are losing a huge proportion of their databases through a lack of responses.

LEGITIMATE INTEREST

Thank the Lord for **LEGITIMATE INTEREST!** Not every use of data requires consent. As a charitable not-for-profit membership organisation much of what we do as churches requires the appropriate use of data to fulfil our charitable aims and objectives. Legitimate interest is a perfectly adequate and legally justified rationale for using and storing data as long as this is recognised in our documentation and procedures. For example, to operate a team rota you need to hold the contact details for team members, and depending on the circumstances you may need to share those details with other members of the team. This is covered by legitimate interest and therefore consent is not required. A basic data risk assessment should be conducted where data is processed under the rationale of legitimate interest, i.e.

a) Identify your legitimate interest. What is it?

b) Prove the necessity of processing data. (Without it, I couldn't do the following…)

c) Put in place any safeguards (reasonable expectations) to protect the data, control the distribution, keep it up-to-date, remove people from lists when needed, etc.

PROCESSING

Under GDPR, **PROCESSING** is the term that covers all interactions with our data. If we look at it, or do anything with it we are processing it.

SUBJECT ACCESS REQUEST

SARs existed in prior legislation but the introduction of GDPR will draw attention to them and therefore the number of SAR submissions is likely to increase, particularly where challenging relational factors are in play. Simply speaking, as an individual you have the right to see all the data an organisation holds on you and a **SUBJECT ACCESS REQUEST** is the mechanism by which you can request it. For example, if you walk into a supermarket and get picked up by a number of their CCTV cameras, you can contact that supermarket and ask for a copy of the video footage they hold of you. This is your legal right and they are legally obligated to provide it. The same applies for churches and you should consider the implications of this when you choose what data to store on someone.

UNSUBSCRIBE, OPT-OUT
If people want us to stop communicating with them, there needs to be an easy process for them to request this, to **UNSUBSCRIBE.** It needs to be easy and clear for them to **OPT-OUT** from us emailing them or processing their data. This is particularly important where we are sending out mass mailings (to multiple recipients) such as e-newsletters. We need to consider using proper systems for this (such as Mailchimp or a CMS (Churchsuite)).

SPECIAL CATEGORY DATA (SENSITIVE)
GDPR defines various categories of data which it considers to be special or sensitive. This covers anything about race or ethnic background, political opinion, health status, sexual orientation and religious affiliation. In these circumstances, GDPR wants to see increased care and discretion enacted for this data. Therefore, as churches, we need to take this responsibility seriously as much of our data represents religious affiliation.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)
A Data Protection Impact Assessment is a type of risk assessment used to consider the data protection implications of a new activity or data function. This may cover starting to use a CMS for the first time or installing CCTV. DPIA templates are available on the internet.

Principles of GDPR and Data Protection

GDPR is designed to protect the individual and to recognise that their data (wherever it is) is indeed theirs. It aims to ensure that use of data is:

- Fair, lawful and transparent. Our use of data needs to be well thought through.
- Compatible and specific (limited to an appropriate and defined purpose)
- Adequate, relevant and necessary (the principle of data minimisation)
- Accurate
- Rectifiable (process for errors to be corrected)
- Appropriate for purposes and not retained for any longer than necessary

All of the above is easy to agree with. We should be looking after data in this way, so GDPR is simply appropriate stewardship.

The nitty gritty…. What steps are being taken at St John's to ensure compliance?

This is still an ongoing process but the aim is to complete the majority of the following steps by the end of July 2018:

Step 1: Conduct a Data audit. Find out what data is in existence, where it is, how it is stored and who has access? Make sure the scope of this audit covers everything. All team members, ministry leaders, clergy, trustees etc. If a list, spreadsheet, database, address book or otherwise exists within St John's, find out about it. Document the results and the fact that this audit has taken place. Diarise a review of this audit at a later date, perhaps as part of an annual cycle.

Step 2: Once the audit is complete, **rationalise your data**. Minimise the number of lists and databases in use. We are in the process centralising this data within one single cloud based Church Management system (ChurchSuite). This Data Processor has elements in place to assist us with

GDPR compliance. We can control access via permissions and passwords and no data is locally stored (which minimises the risk of data breach).

• Shut down as many separate excel spreadsheets as possible.

• Remove from public access any paper lists or directories. Any data on paper should be securely stored.

• Minimise the use of Outlook or other email programmes for mass mailings and never email a group (where either consent or a legitimate need to share email addresses hasn't been considered) without using the 'bcc' function. Establish this as the 'culture' within your church. Where e-newsletters are used, have a simple and clear unsubscribe process. (Mailchimp and CMS's work well for this purpose, but bear in mind that Mailchimp will become a data processor for you, if you utilise their service!)

Step 3: Appoint responsible people within your church for specific data roles.

• Every data asset (list or database) should have an Information Asset Owner (IAO) who is responsible for monitoring the data, reviewing it annually (or otherwise), archiving old data, removing people by request and ensuring accuracy. **(This covers hands-on detailed management of data)**

• Gillian Mannouch is the Data Lead who will respond to any data requests from members of the general public. **(This role represents Organisational management)**

• We need to appoint a member of the PCC as a Senior Information Risk Owner (SIRO) to champion the care of data in St John's and to keep our responsible people accountable. **(This role represents our governance and accountability function)**

There are other data roles which we may wish to have, but the three listed above should adequately service our responsibilities and demonstrate that we take these seriously.

Lots of attention is given to the role of a Data Protection Officer, however most smaller organisations and therefore most churches will not have one. DPOs need to be independent of our management structure and they operate with autonomous authority. They are usually either designated employed roles or outsources. Therefore, for the context of most churches they are cost prohibitive and ultimately not required.

Step 4: Consider appropriate security precautions (on data files, paper and digital)

• We are in the process of implementing a professional church management system (ChurchSuite) to store and process our data with the use of passwords and hierarchical permission structures. Storing data in a centralised, secure, cloud based database will not only improve operational efficiency but will protect data and simplify our data protection processes.

• Consider how we communicate and send mass mailings. Try and do this via a databased driven system as opposed to via individual mail clients.

• Store any paper files (DBS records, child registration forms, electoral roll forms, welcome cards etc.) in a lockable and ideally fire resistant filing cabinet. Don't retain files for longer than needed. See https://www.churchofengland.org/sites/default/files/2017-11/care_of_parish_records_keep_or_bin_-_2009_edition.pdf for guidance on statutory requirements, but also consider an internal policy for all items of data. How long should we keep welcome cards or Christianity Explored signups?

• Should we consider stopping publishing personal details of individuals in newssheets or on websites? Is it worth the hassle of obtaining consent?
• Make sure that we don't have any personal data on display or accessible on a Sunday. Our church is a public building and it is not safe or sensible to have this data freely available.
• Where possible, store all data on secure central servers or the cloud. Always password protect data files. Don't keep personal data on USB disks.

Step 5: Analyse your audit and **consider what data processing falls under 'legitimate interest'** and what requires consent. Document this and perform the necessary simple risk assessments. Reflect our outcomes in our privacy statement (see below).
• Apply common sense – don't make this harder than it needs to be.
• If we need to process data to operate and fulfil our legitimate charitable aims and activities, our processing of data is probably covered by legitimate interest
• It is legitimate to communicate with the members of St John's about the activities of St John's. This is part and partial of being a member.
• However, if someone has just filled in a welcome card we should only answer their initial questions and invite them to appropriate welcome events within an agreed period of time from their initial enquiry (our decision to make but perhaps circa 3 months?). Don't treat them as a defacto member and start asking them for financial contributions or to sign-up to the cleaning rota. Similarly, if someone attends a one-off event, gets married at our church or signs-up to an Christianity Explored course, make sure we recognise why we have their personal data and deal with it accordingly (for that purpose and immediately related purposes only). We don't have carte blanche.
• Should we have a process for monitoring engagement levels in church life? If someone stops being part of our church, how quickly do we notice and what are we going to do with their data? Ideally, this should be picked up and their data archived within 3 or 6 months. Church Management systems can often aid this function.

Step 6: Where consent is required, and we don't already have it, provide a simple method to gain it. This needs to be clear, specific and demonstrable.
• We need to beware, if we don't have consent to email someone, we shouldn't email them to ask for their consent. Catch 22 – you'd be immediately breaking the law. Electronic communication is governed by PECR (Privacy and Electronic Communication Regulations. https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
• We are utilising ChurchSuite to provide user access to database records and personal control of privacy and consent settings.
• We will update our welcome card, electoral roll, and Who's Who forms to incorporate specific consent wording. We will reference that data is used and stored in accordance with our privacy policy. If we would like permission to contact them to promote church events (run under the auspices of your leadership, which we feel may be of interest to them), we will make this explicit.
• We will make sure, in practice that we don't step outside of our consent parameters when communicating with people.

• We will ensure everyone has a clear and easy option to unsubscribe from communication and if they wish to revoke their consent or would like to be 'forgotten' it is clear who they should speak to.
• If we believe we already have received consent, there is no need to renew it, but we should communicate to all members with the introduction of GDPR, reference our privacy policy and emphasise the opportunity to opt out and update/change their own privacy settings.
• The GDPR says children under 16 cannot give consent (although this will be reduced to 13 in the UK), so we will have to obtain consent from a parent or guardian. We will need to be able to verify that person giving consent on behalf of a child is allowed to do so.

Step 7: We have drafted a Privacy Statement, encompassing our entire use of data. This needs to be approved by the PCC. Once approved:
• It will be available on our website and we will reference it on all data collection forms. This will also be available in our church office in paper form and on the noticeboard displayed at the back of church.
• Once written and enacted, we must stick to it!

Step 8: The staff team and other ministry leaders will be trained by talking them through this guidance sheet and our privacy policy. Training our team is part of our compliance with GDPR. We must make sure everyone knows who is responsible for data protection within St John's and what level of practice everyone needs to adhere to.

Step 9: We need to **implement an annual process of review**, archiving, data cleansing and house-keeping. GDPR compliance is not a one-off task, it is an ongoing commitment and this needs to be followed and documented. Ideally we should pick an appropriate time of the year (when it is mythically quiet!) to perform this review.

Step 10: We need to put a **plan in place in case of emergencies or data breach**. The ICO will like to see that we have a plan in place with appointed persons who understand their responsibilities in the event of their being an issue. The policy should be practical and simple. This need not just be a paper exercise – it will help us respond to issues coolly and calmly.