

Welcome to the

GDPR Training Day

20 March 2017



What we're here to do

- Understand the law
- Think about the data we hold (audit)
- Get practical help for implementation
- Make a plan



Practicalities

- Fire
- Facilities
- Food
- Phones
- Faith



Theology

- Respect, uphold the dignity of, & protect those made in God's image
- This includes taking care over the way that we collect, hold, use and dispose of information about people



Why GDPR?

- Poor fundraising practice by some organizations
- Serious data breaches (eg TalkTalk)
- Ever increasing capacity to retain data
- The right to be forgotten



Working together

- Church of England contains thousands of churches, parishes and other bodies
- All are responsible separately for implementation as legal organizations
- Diocese is providing support, assisted by national church colleagues



Mapping the terrain

- This is new legislation. Some aspects of interpretation will be defined by Case Law.
- The law is 'one size fits all', but the solutions may vary from one parish to another.
- The Diocese can help, but parishes need to do some work on this.



What are we dealing with?

- Solid ground – safe or broadly safe
- Middle ground
– moderate risk
- Shaky ground
– higher risk



What you can expect from us

- Today
- An overview of the main issues
 - Help to start a data audit
 - Privacy notice and policy templates
 - Mapping out a compliance plan
- Ongoing
- Telephone support and advice







What is it?

- Replaces the Data Protection Act 1998
- New European-wide legislation
- Will be part of UK legislation through the Data Protection Bill – same commencement date

The slide contains a title 'What is it?' followed by a bulleted list of three points. At the bottom left is a colorful tree logo, and at the bottom right is the Diocese of Leicester logo.

When does it start?

- Officially on 25 May 2018
- Now!
- Planning required NOW!



What is data?

- Anything that identifies an individual
- May vary: -
 - Laura Smith - ?
 - Lady Laura Smith - Yes
- Date of Birth, Baptism, Marriage, Death, Funeral
- Address, Telephone no, email address, partner, etc
- Photograph(s)
- Readily accessible filing system



- Plus
 - Religious belief - extra sensitive data
 - Other data (see later)



Principles for dealing with data

- Dealt with lawfully, fairly & with transparency
- Collected for a specific purpose and only used for that purpose
- Adequate, relevant, necessary
- Accurate and kept up-to-date
- Identifiable only as long as needed
- Protected against misuse, unlawful access / processing &/or loss / damage



Key Actions

- Data Audit
- Privacy Notice
- Consent – where needed
- Check and delete old / unnecessary information
- Data Security



- Establish retention periods
- Inform & train
- Respond to Subject Access Requests



Rights of Data Subjects

- To request a copy of personal data held about you
- To request the organisation corrects any inaccurate or out of date personal data
- To request deletion of personal data where it is no longer necessary to be retained
- To withdraw consent to processing at any time



- To request data portability
- To request a restriction is placed on further processing where there is a dispute in relation to the accuracy or processing of your personal data
- To object to the processing of personal data, (where applicable);
- To lodge a complaint with the Information Commissioners Office (ICO).



Key Principles

- Fair
- Lawful
- Transparent



Fair

- How was the information obtained?
- Reasonable use of data under that circumstance
- Use for collection = use of it now?



Legal

- Performance of contract
- Legal Obligation
- Vital interests of subject or another
- Task carried out in public interest / official authority
- Legitimate interests of controller
- Consent



Legal – Sensitive Data

- Explicit consent
- Legitimate interests of not for profit body with religious aim AND
 - Appropriate safeguards
 - Applies to members, former members, people who have regular contact



AND

– No transfers to third parties



- Already made public by individual
- Necessary for:
 - Employment
 - Protection of vital interests
 - Establishment, exercise of defence of legal claim
 - Substantial public interest on basis of legal requirement
 - Preventative or occupational medicine
 - Public interest in area of public health
 - Archiving in public interest, scientific or historical research, or statistical purposes



Consent

- Article 4 requires consent to be: -
 - Freely given
 - Specific
 - Informed
 - Unambiguous



- Demonstrable
- If other matters involved, must be clearly distinguishable
- Right to withdraw at any time
- If freely given, UTMOST regard to whether consent is conditional for provision of service/performance of contract if personal data itself not necessary for provision of that service/contract



Transparent

- Is use of that data clear and obvious?
- What was the data subject told?
- What is in your Privacy Notice?
- What is in the Information Commissioner's Office registration (if applicable)?



Why do we hold data

- Legal requirement
 - Baptisms, Wedding & Funeral records
 - Electoral Role
 - PCC Officers & Members
- Archive – History
 - May cover some of the above as well



Exercise One

Complete the template for your parish(es)



What data do we hold?

- Baptism information
- Wedding information
- Funeral information
- Financial information
- PCC information – Agendas, Minutes
- Pastoral Information
- Safeguarding information
- Other information



Who holds that data?

- Clergy / Reader / Pastoral Assistant
- Administrator
- D/PCC Secretary
- D/PCC Treasurer
- Safeguarding Co-ordinator
- Messy Church leader
- Sunday School team
- Baptism / Bereavement Team



- Electoral Roll Officer
- Parish Magazine Distributor(s)
- Flower Arrangers (Rotas)
- Churchwardens (Rotas, etc)



- Incumbent – Data Controller
 - Associate Minister, Curate, Reader
 - Under Incumbent's authority
- PCC – Data Controller



Data Protection Documents

Andy Brockbank and Claire Bampton



Overview

This session is about the documents you need to demonstrate that you are complying with GDPR.

Keep a record of everything you do to be compliant. This is your evidence if asked to provide it.



Privacy Notice

A privacy notice tells your data subjects about what you are using data for, where it's held, who you share it with and who they can contact in the organization.



Template Privacy Notice

- Produced by the national church
- Available from
 - www.parishresources.org.uk
 - Link from diocesan website
 - NB. Our version is slightly amended
- Don't just adopt it – check it meets your needs.



Consent form

- Not to be confused with a privacy notice!
- A consent form is used to get people's agreement to process their personal data
- Only seek consent if the use is not covered in another way (eg legal necessity, legitimate purpose)



Template Consent Form

- Data collection form
- How to contact people
- For what purposes
- Only seek consent where you need it!
- May need different versions



Policies

You don't have to have a general Data Protection Policy, but people expect it

Some policies are necessary, eg Data Breach, Data Retention

'Bring Your Own Device' Policy will be necessary for most churches



Template Data Protection Policy 1

- Baptist Union template available from www.baptist.org.uk/Groups/302154/Data_Protection_and.aspx
- Policy statement (1.1) – why you use data
- Application to you (3.)
- Basis for using data (6.2) and ‘special category’ data (6.3)
- Security of personal data (12.)



Template Data Protection Policy 2

- Sharing information (16.)
- Data processors (17.)
- Data Protection Impact Assessments (19.)
- Data breach (20.)



Data Retention

- Church of England Records Centre guidance on retention periods



Bring Your Own Device

- Some churches hold all data on private devices
- Take sensible precautions
- Extra care with sensitive data



Activity

Look at the examples of documents on your table.

What questions do you have about them?

Can you adapt them for use in your parish?



Questions



Data Protection and 'Marketing'



Overview

This session is about how we can use the different methods of 'marketing' whilst being compliant with GDPR



What does 'marketing' mean for parishes?

The ways we publicise church activities and services to individuals in our congregations and communities.

It includes communicating with people about financial giving to the church and fundraising.



Q: Does it involve personal data?

If not – GDPR doesn't apply.

E.g. Easter cards with service details, not named or addressed

E.g. Posters or fliers circulated with the local newsletter

If yes – same principles of GDPR apply



Methods of communicating

- Email, texting (SMS), messaging apps e.g. WhatsApp

Need to have consent to use

- Phone calls

Doesn't come under GDPR – already governed by regulations around 'Telephone Preference Service' (TPS)



Methods of communicating

- Post

No single answer.

Need to consider 'legitimate interest' and 'reasonable expectation'

- Envelopes that are unnamed and unaddressed – no use of data, GDPR does not apply



Post: named and addressed

‘ You can provide members of the Electoral Roll, or other regular members of the church, with physical packs of materials assuming that you have registered a “legitimate interest” in your privacy notice. ’

Parish Resources: GDPR & Giving Reviews



Legitimate Interest

‘ ...can be used where there is a relevant and appropriate relationship between data subject and the controller. ’

Parish Resources: GDPR & Giving Reviews



Reasonable Expectation

‘ anyone who has proactively joined an Electoral Roll should be aware that churches fundraise, and should thus have a “reasonable expectation” that parishes should engage in this activity. ’

Parish Resources: GDPR & Giving Reviews



Reasonable Expectation

‘ where individuals have **subscribed** to the Parish Magazine, you can include the giving pack as a supplement to the magazine ’

Parish Resources: GDPR & Giving Reviews



Discussion Around Tables

- Think of one relevant example in your parish
- Think through whether you need to change how you do it
- What is your reasoning?



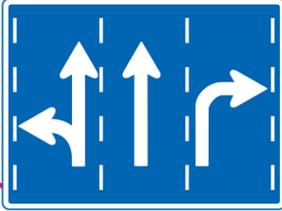
Plenary

- Questions arising from your discussions



Where do we go from here?

Rupert Allen and Andy Brockbank



Overview

This session is about working out what you need to do and builds on the work done before lunch on data audit.

First step to compliance is having a plan in place – by 25 May 2018.



Consider your strategy

1. Avoid GDPR as much as possible
2. Stick to 20th century methods
3. Embrace technology and get consent



Privacy Notice

- Every parish will have to issue this to some people
- Needs to be issued to everybody who is a data subject
- Can send a summary and link to the full version



Data collection (consent) form

- Who needs to receive this?
- Consent not needed if you have to process data for a legitimate interest
- Double consent for 12-16 year olds



A mission opportunity?

- Making contact – ‘the law is changing’
- Showing appropriate care – ‘we’re looking after your data’
- Using face to face contact



Data security

- Who holds data?
- On what device(s)?
- Do they password protect information?
- Do they need training?
- What are the risks if information leaks?
- How will we know?!



Access to information

- What is a SAR?
- Would you recognize one?
- How will you respond within 30 days?



Action planning

- Talk through your next steps
- You don't have to do it all at once
- Focus on the key areas



Questions and feedback