
GDPR FOR PARISHES

What is Data Protection?

- Data Protection is about avoiding harm to individuals by misusing or mismanaging their personal data.

So if you collect, use, or store personal data then the Data Protection Act applies to you.

The original Data Protection Act was in 1988.

It introduced eight data protection principles

1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. not transferred outside the European Economic Area without adequate protection

In the last 30 years, technology and its use have has changed. It's time to make sure that we are all following the original principles (which we should have been all along).

In addition, some recent news stories
- Loss of personal data e.g. by large corporations like UBER,
- Sale of charity mailing lists from one charity to another

Now neither of these may be relevant by parishes – so our difficulty is to find a way through the maze of legislation that is not really written with parishes in mind, but larger organsiations.

Parishes need to see data protection as part of the legislative framework they operate in, part of being a good citizen, like H&S or safeguarding

Our approach is to do a good enough/reasonable job: proportionate to the size of the parish and its resources

The New GDPR, from 25 May 2018

What's the same

1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. not transferred outside the European Economic Area without adequate protection

It's the eight principles again

The New GDPR, from 25 May 2018

What's the same

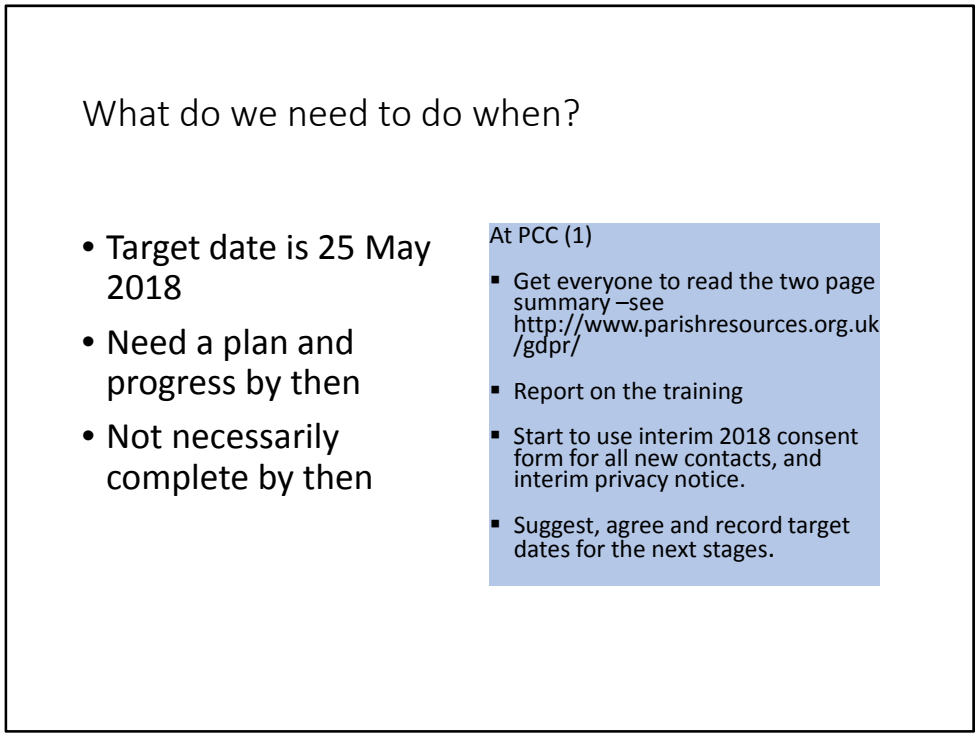
1. used fairly and lawfully
2. used for limited, specifically stated purposes
3. used in a way that is adequate, relevant and not excessive
4. accurate
5. kept for no longer than is absolutely necessary
6. handled according to people's data protection rights
7. kept safe and secure
8. not transferred outside the European Economic Area without adequate protection

What's new

- Processed lawfully, fairly**, transparently**
- Collected for specified, **explicit and legitimate** purposes
- Adequate, relevant and limited
- Emphasis on demonstrating compliance
- Right to be informed
- Right to be forgotten
- Report data breaches
- Free access, one month

The real change is an emphasis on

- Informing people in a way they can understand
- Demonstrating – not just being compliant (think Ofsted)
- New rights in certain circumstances e.g. to be forgotten
- New obligations – to inform, to report breaches, to provide free access within 30 days: not charge and provide in 40 days.



Regulations take force 25 May 2018
The ICO is interested in improving standards and awareness, not imposing big fines.
We are suggesting that parishes need to make a plan and a start.

Our method for dealing with the accountability is to use PCC (or Deanery Synod) Minutes to provide an account of what we are doing. There are other ways, equally valid, but we are suggesting this as one way through the regulations. If people wish to do this, this talk will show 4 sets of minutes documenting progress towards compliance.

Or at Deanery synod standing committee

At the first PCC

Make sure that attendees know about parish resources website: the two page doc can be found there.

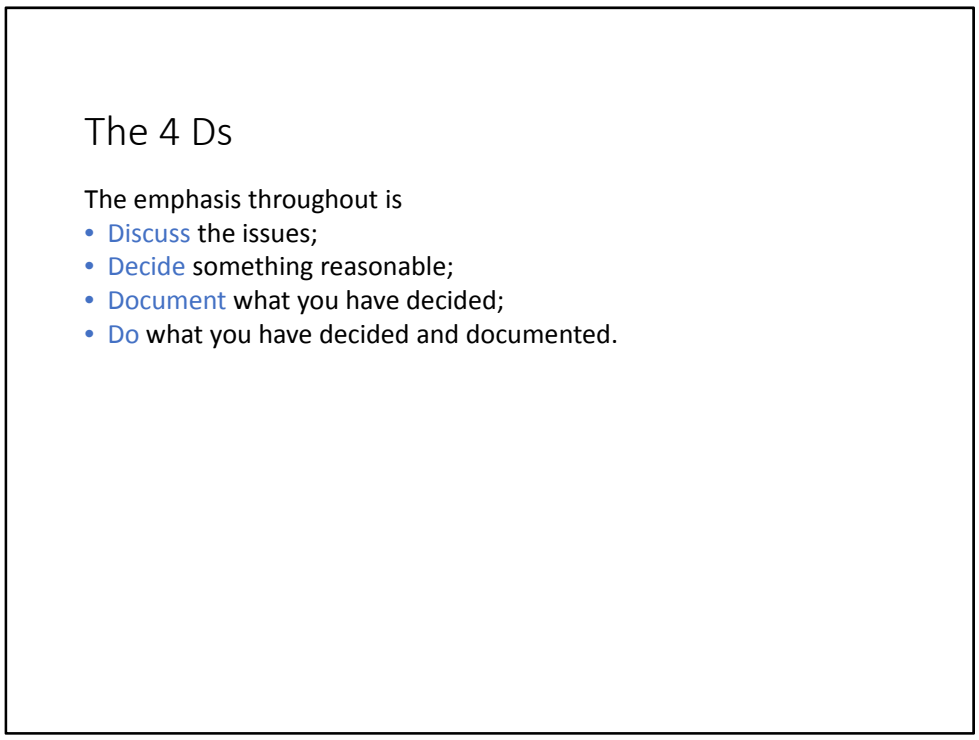
Start to use interim 2018 consent form, and interim privacy notice
There are two consents forms

* one longer one for “members”
* and a shorter one for “friends”/ contacts

Privacy Notice

- put it on the website
- Put it on the church notice board next to other legal docs such as the insurance certificate
- If no church building, laminated on welcome table
- Can occasionally draw attention to it in parish mag!

PCC members are not liable individually, so long as they follow the guidance of the PCC. But the PCC must provide guidance – and if it is reasonable, and the PCC has taken advice/been on training, then they would be OK.

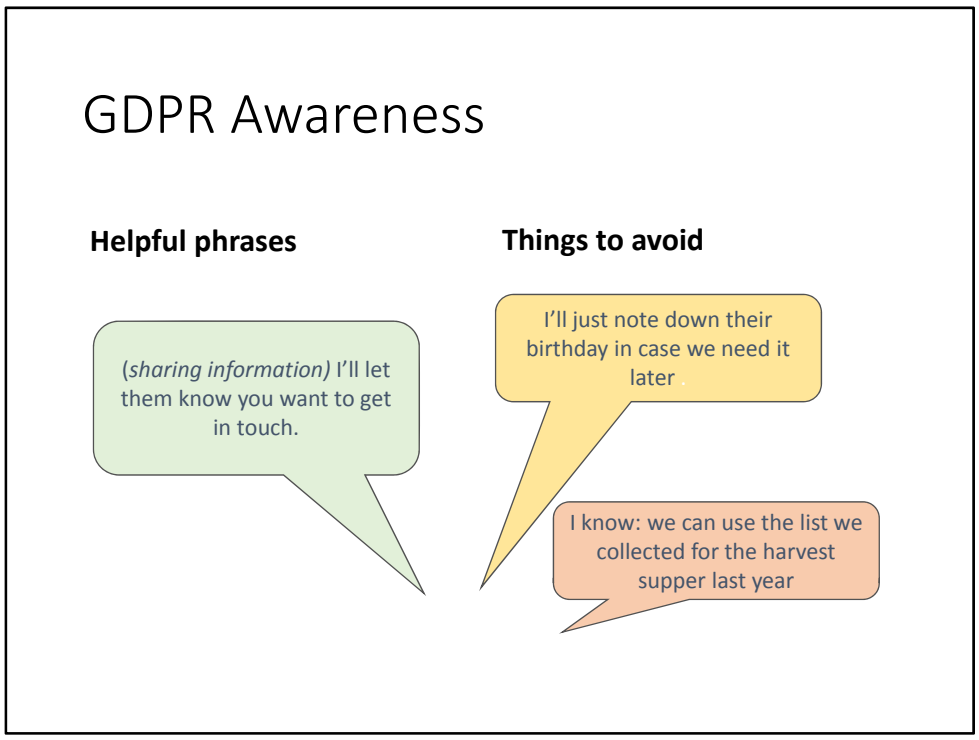


This is the trainer's answer to any hard question!

The doing is important – telling people what the new method is.

If it subsequently becomes apparent that this was the wrong decision, you can revise it.

The purpose of this is for the PCC to be **data aware**, to make **demonstrably** (because minuted**) deliberate** (because issues considered) **decisions** (and choice made), not allow things just to happen (treasurer keeps finance details on laptop shared with teenager!) without thought.



People attending the course have two roles.

One is to encourage compliance by going through the process.

The other is to raise awareness generally among church members about the data protection principles. Here are three examples to share and get people thinking:

a) Do you have a parish office? Can I phone up the parish office and ask for another member's phone number if I need to get in touch to do something church related, such as organise next week's Sunday school? What does the parish administrator say?
This usually leads to some discussion about what phone numbers are public e.g. Vicar and Churchwardens, and whether people can/ need to consent to having their numbers shared. Also, what happens in parishes that have a printed directory of names and contact details.]

b) Suppose you had a harvest supper for members and friends, and are now planning a valentine's line dancing evening (or other topical example). Can you mail out to all the people who came to the harvest supper and invite them? Answer – it depends – did they agree to be mailed about social events generally, or just the harvest supper?

c) Suppose your parish runs a lunch club for the elderly, and has a list of names and contact details. Someone thinks that *in the future* they *might* like to send birthday cards to members and so writes down everyone' date of birth. That's not OK, data just in case. It is OK if you *already* are sending out birthday cards, or to *ask later* when you are about to start.

What is a Data Subject?

A human being

Living, identifiable individuals

Personal data – anything that could be used to identify someone.

- Probably: name, address, email, phone number(s)
- Maybe the parish has: bank details, photographs

Important to notice

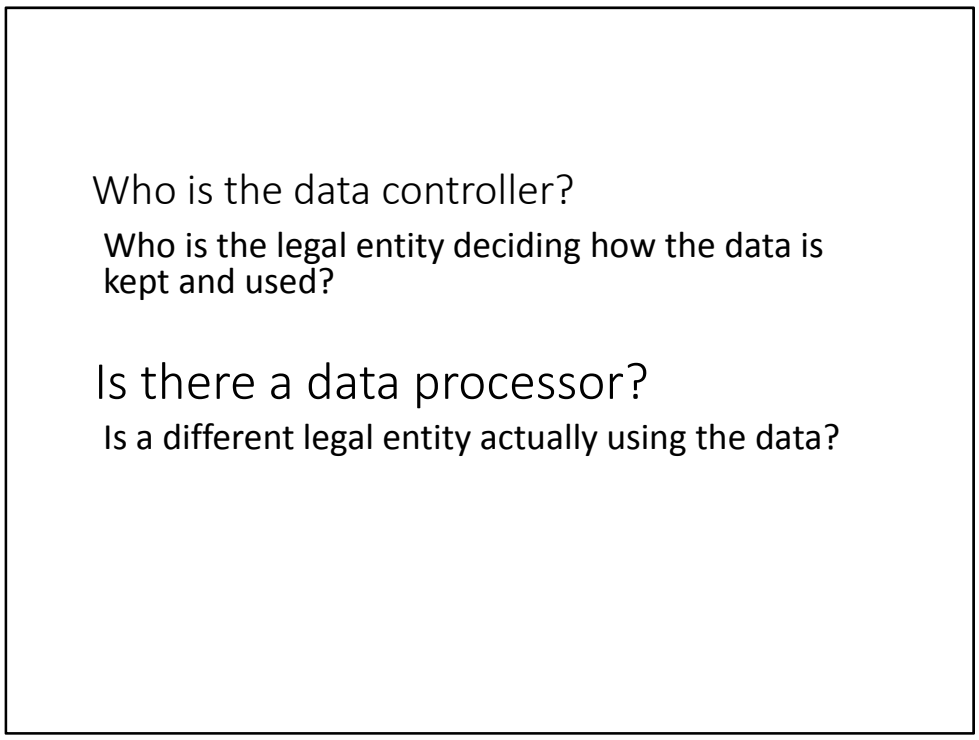
- Dead excluded
- Any data that identified people is included: obviously names and contact details
- Bank details of employees, sometimes givers
- Photos of one person with a name underneath **is** personal data. A group photo with the caption "Petronella Spivey and friends" is **not**, because a stranger would not know which one is Petronella.

Ask for suggestions about who they have data about?

This usually leads to a discussion about people who provide services for the parish: the photocopier service engineer, the person who mows the graveyard. Although there is a distinction between corporate entities (e.g. Photocopier Services incorporated) and sole traders, strictly speaking the name and mobile of the service engineer is also personal data.

It is also worth thinking about people who hire the hall. Obviously a parent hiring a hall for a party is personal, and it is possible you have corporate hirings, but brown owl's details are personal even though she is part of a larger

organization.



Legal definitions

Data Controller: making the decision about what data to collect and how it is used.

Point out that the PCc and the incumbent are separate legal entities. (Although the incumbent is a member of the PCC) We are still waiting for good advice from the national church about incumbents.

Also awaiting clear advice for multi parish benefices with a benefice administrator responsible for several parishes. The 4Ds are relevant, also the possibility that a multi-church parish can simplify compliance in all legal areas.

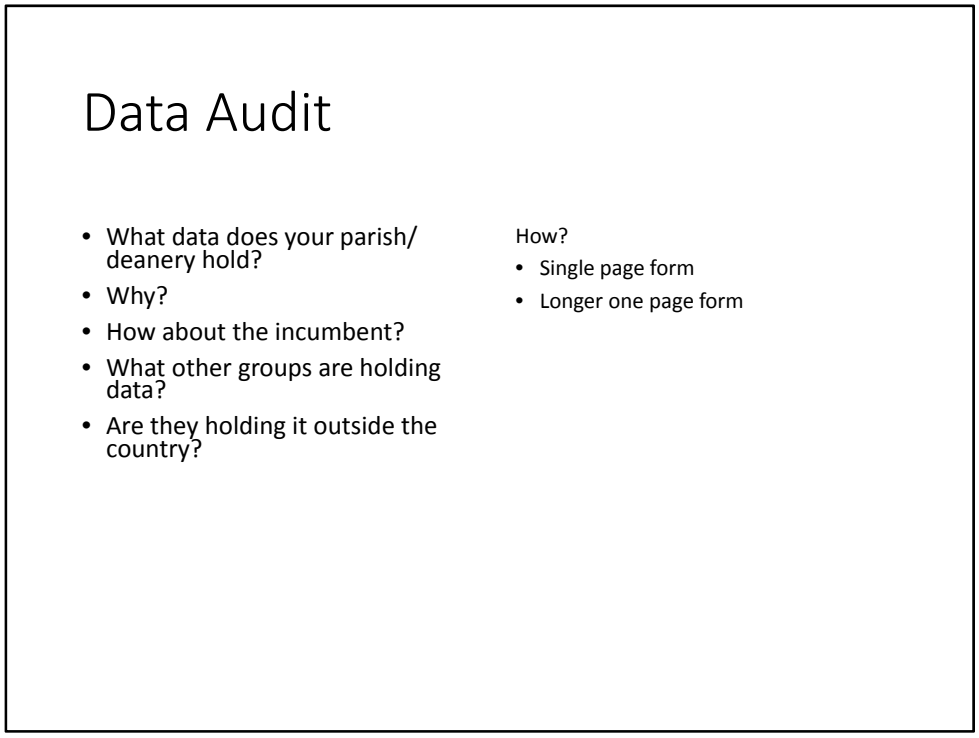
Does the data pass to another legal organisation for further work – this is the data processor. Both are responsible for the data being properly handled.

Examples of transfers for parishes: payroll data.
Maybe also: cloud storage.
Where the parish is a controller, and another organisation is the processor, then the data controller (parish) is responsible for making sure that the processor has proper data protection policies in place.

Ask if the parish has a funeral ministry (people will agree) – point out that when a bereaved person contacts the funeral director, the funeral director will collect the contact data, and pass this on to the parish. The Funeral director is the data controller and the parish is a data processor i.e. a separate legal entity. The controller should be telling you how they want the data handling and that after the funeral the data will need to be destroyed.

Show the one page contact form and point out that they will need to say to the bereaved at some point that the parish likes to invite them back for all souls and needs their permission to do so – a small post card to complete at this time is sufficient.

.



First step for parish is data audit.

Each table to work on these questions for 15 minutes

What data does your parish/ deanery hold?

Why?

How about the incumbent and the rest of the ministry team, retired clergy

How to record

Use the parish resources spreadsheet, with one row for each item,

Or if preferred, one item on each page

Or a blank sheet.

During this session, invite people to refreshments.
Also work round some of the tables answering individual questions.

Write up on paper flip chart what people have found. A typical list looks like this

Members
Friends of the fabric
Employees
Electoral Roll
People on prayer rota
Groups: flowers, bell ringers, choir, home groups
Mailing list for parish magazine
Hirers
Contractors
Registers
People coming for occasional offices (BMD)
Service users (mum and tots, dementia lunch etc.)
Youth group members

Encourage people to use this list to augment their own audit. (and photo it)
Suggest people also use Keep or Bin, despite is age, is a useful source of possible data.

Where are my biggest risks?

- Which is the most sensitive data?
- Where is the greatest likelihood of error?
- Where is the biggest risk?

Explain that

- People need to identify their biggest risks as follows

- Which data is the most sensitive / embarrassing. We are using a three point scale at CHO

A potentially harmful to the life, financial interests or reputation of the individual concerned
B embarrassing distressing and unprofessional, but not as serious as A
C the information is already in the public domain.

Which data has the least rigorous processes surrounding it?
A confident that it is secure from unintended use
B fairly certain that it is secure from unintended use or loss
C concerned that there is a real risk that it might be accessed by someone who should not access it.

The biggest risk is where you have answered AC, then AB and BC. This is where parishes are going to need to focus their efforts, on improving their processes. This will have the effect of raising awareness/ tightening

procedures generally...

Do we need to register with the Information Commissioner?

- You do not have to register if organisation was established for not-for-profit making purposes and does not make a profit or if your organisation makes a profit for its own purposes, as long as the profit is not used to enrich others. You must:
- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the organisation or have regular contact with it;
- only share the information with people and organisations necessary to carry out the organisation's activities. Important - if individuals give you permission to share their information, this is OK (you can still answer 'yes'); and
- only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration

Check at
https://ico.org.uk/for-organisations/register/self-assessment/ (Probably not)

The questions to determine if you must register are

1. Do you use CCTV – if yes, you must register says the ICO
2. Are you processing (=any of obtaining, recording, storing, updating, sharing) info – if no, then you need not register
3. Do you process the info electronically?
4. Is your organisation responsible for deciding how the information is processed?
5. Do you only process information for one of the following purposes?
   - Judicial functions;
   - domestic or recreational reasons (i.e. information relating to a hobby); or
   - to maintain a public register (i.e. you are required by law to make the information publicly available)
6. Are you a not for profit that qualifies for an exemption (membership, activities, sharing only with consent, only keep current members) ←- this is the get out for most parishes

Do we need to pay a fee under the Digital Economies Act?

"Will there still be exemptions under the new fee model? Yes, what these exemptions will be has yet to be confirmed by DCMS but we expect them to be similar to those under the current regime."

Micro organisations (Maximum turnover of £632,000 or no more than ten members of staff.) will pay Fee: £40 (or £35 if paid by direct debit)

To register with the ICO:
https://ico.org.uk/registration/new

It costs £35 at the moment and last for a year. If you register now, before GDPR, you are assured that you will not need to register again till next year.

Next steps

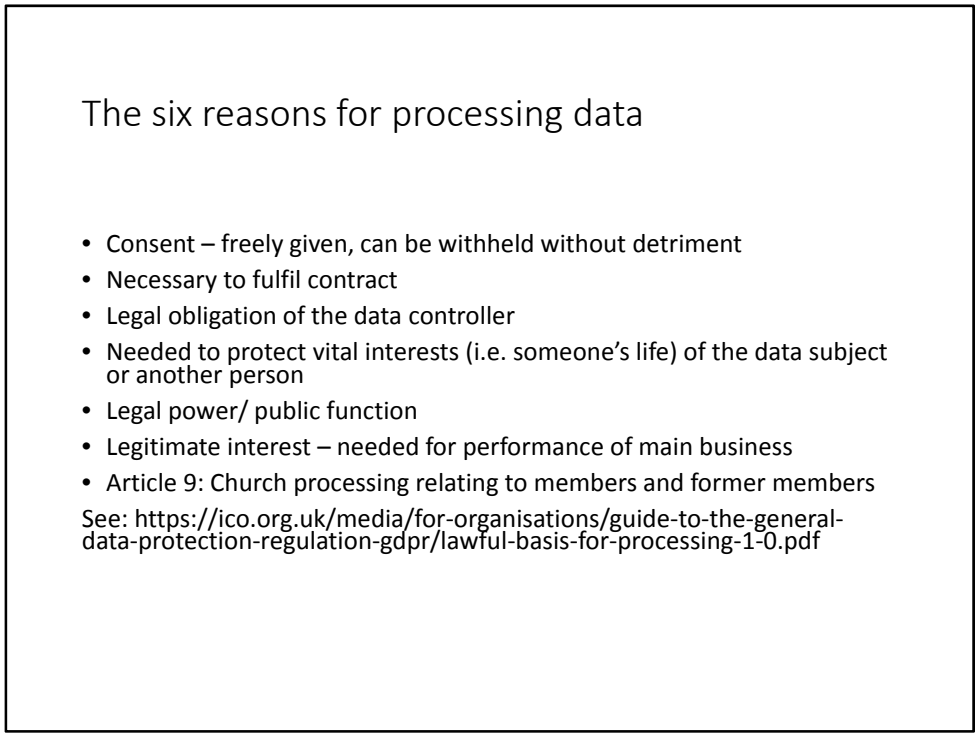
At the next PCC (2)

- Note the work on the data audit
  (Include a copy of the audit in the minutes book)
- Make a commitment to review the audit after a reasonable period of time (2-3 years)
- Agree whether to register with the ICO or not, record the decision, and follow up.

Next steps

Legal basis for data holding, privacy notices and consent forms

Can combine this step and previous.



Or lawful basis

There are six reasons given in the act for holding data, and most of the discussion so far has revolved around consent.
But actually there are all these, and no one of them is better than another; you should pick the one that is most appropriate.

The definitions are tricky, so a useful document (referred to on the slide) is included in the handout.

Choose one – the most appropriate

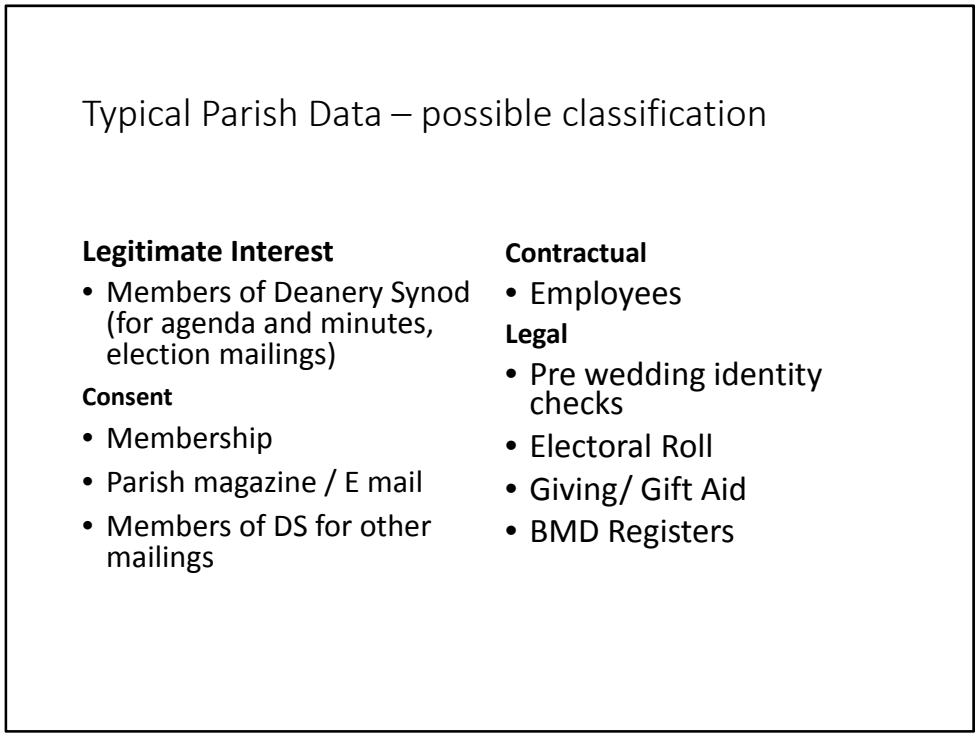
This depends on your specific purposes and the context of the processing. You should consider which lawful basis best fits the circumstances. You might consider that more than one basis applies, in which case you should identify and document all of them from the start.

Consent – freely given, can be withheld without detriment. Forms must be kept (or no audit trail)
Necessary to fulfil contract – employees, weddings?
Legal obligation of data controller – tax, registers,
Legitimate interest – needed for performance of main business, Electoral roll

(CRR) weddings?
Needed to protect vital interests – can release a phone number/ address if you think life is at risk,,,,
Legal power/ -- weddings
public function "the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law."

And the seventh one:
Article 9: Church processing relating to members and former members: if you just have lists of rotas etc. **and you do not share the information outside the church** then you do not need consent and can rely on this. But is doesn't work if you have any sort of mailing list that you use to invite people – only to maintain what is happening. This may help small churches (but they will still need to tell people that this this what they do.)

How do we decide which lawful basis applies? Useful handout as shown included in handouts.



A while ago, I came up with this list and categorised the main legal reason like this.

One way to do the feedback is to put this up and ask what people think.

Any difficult question, go back to the 4Ds (Discuss, Decide, Document, Do)

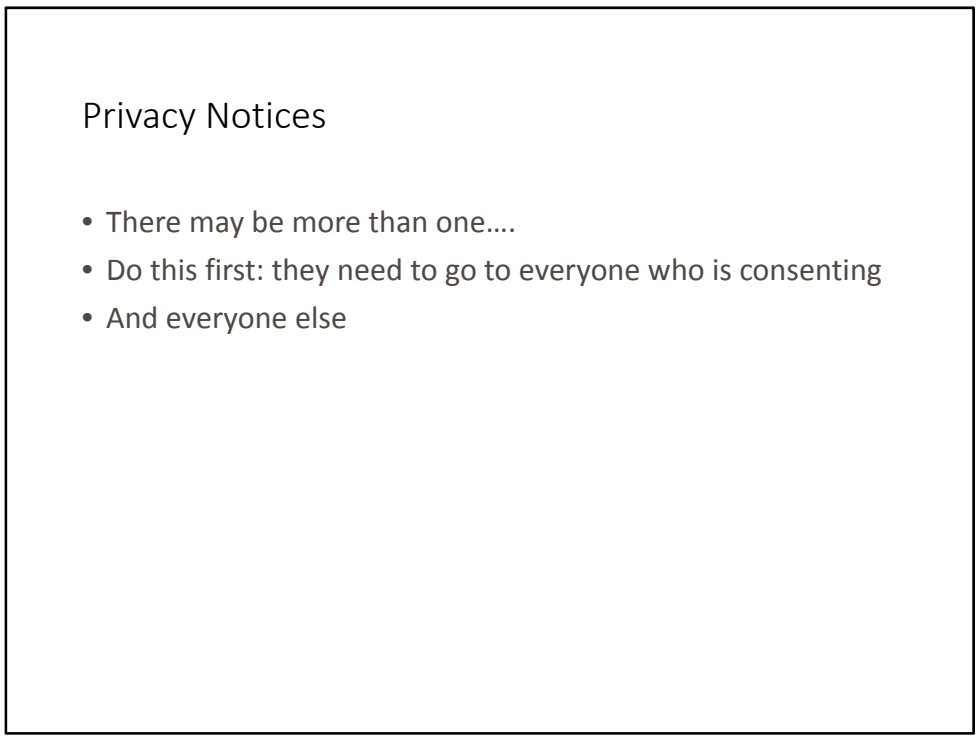
Important Fact about Electoral Roll

No consent is needed for electoral roll – it is a legal requirement. It is also a legal requirement to display it in church. You do not have to display the addresses,, and if you are displaying addresses, now may be the time to stop.

Lawful basis and individual rights

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	X but right to withdraw consent
Contract	✓	✓	X
Legal obligation	X	X	X
Vital interests	✓	X	X
Public task	X	X	✓
Legitimate interests	✓	X	✓

Point out to people that this table appears in the ICO document and explains whether people can object or have the right to be forgotten. This won't take long.



Privacy Notices

The important thing to get across is that now you know what data you hold, and why, you can write a privacy notices that explains this.
Parishes may need more than one, but this may be time consuming.

Transparency means you can't really write vague statements like "We retain your data for as long as it is useful" or "in accordance with local procedures". You must be specific. But you can say, "We retain data according to the following table" if that is helpful in reducing the number of privacy notices you need.

Privacy notices should go on website and official notice board, also to people consenting (otherwise how do they know what they are consenting to?) (See earlier slide about privacy notices)

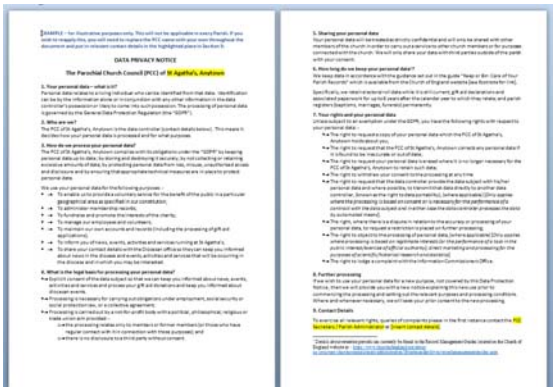
Privacy Notice

One needs to be accessible with your consent form

And on website

And needs to be reviewed periodically.

Interim privacy notice



Useful information about variations can also be found on parish resources website.

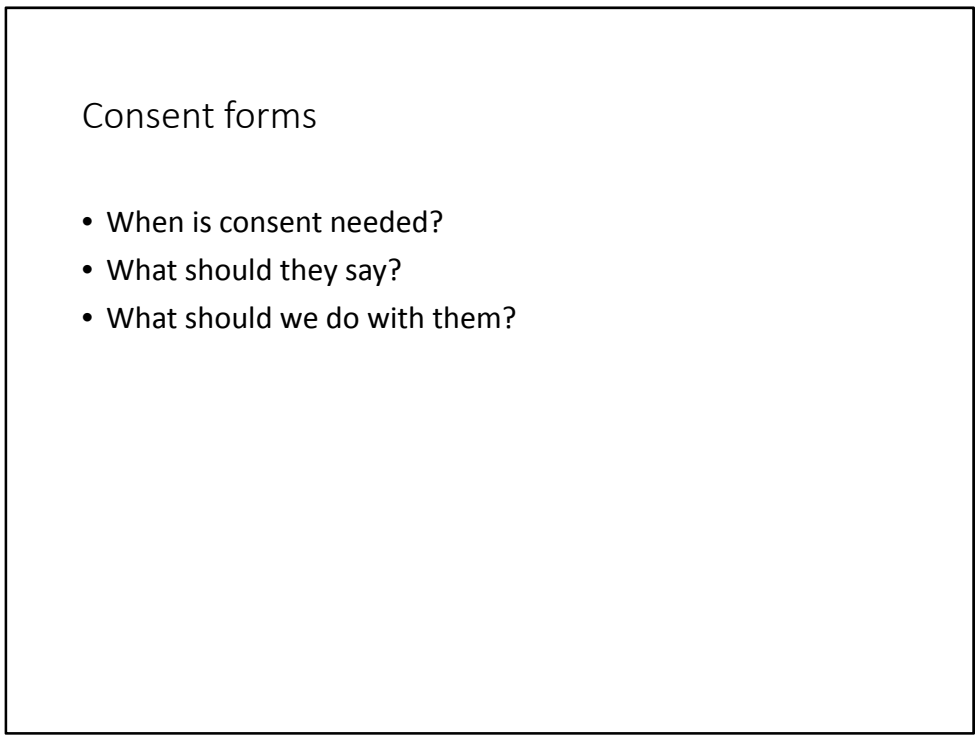
Parishes may want to adjust it following their data audit.

Sensitive data

Religious belief is sensitive, hence the additional wording:

- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided: -
  - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes); and
  - there is no disclosure to a third party without consent.

Don't take this para out.



When?
Only if the legal reason is consent. Go back to your audit. No consent needed for contracts, legitimate interest etc.

What should they say?
Collect only the info you need
U13s need consent of parents – over 13s can consent (but you need to provide info in age appropriate language) (possible youth group activity?), but if you are holding parents contact details, you will need to tell parents anyway.

What do we do?
It is sufficient for forms to be returned by email.
They must be kept – can't just transfer the date they were received to a database/spreadsheet because then there is no audit trail.
But can be kept as scans, emails, anyway you can find them.
Paper should be kept in locked file.
Destroyed on request/ when person dies or moves away. -- best to say this on the form.

Back consent
If you are relying on consent, will need a programme of "back-consenting".

This could be over a time period – go forward with your interim and then newly designed consent forms, but eventually, all members will have to consent.

The Electoral Roll will be rewritten from scratch next year in 2019. You might consider putting a consent form on the back of the standard unchanging ER form and collecting them at the same time. Or you might think that this is not soon enough. Again, it is for the PCC to discuss, decide, document, do.

At the next PCC (3)

- Record the analysis of the data audit.
- Agree local privacy notice to replace interim one, make date to review.
- Record the plan for displaying privacy notices
- Agree local consent form to replace interim one
- Record the programme for collecting necessary consents (including all existing members and contact)
- Start to develop local procedures

Additional Considerations

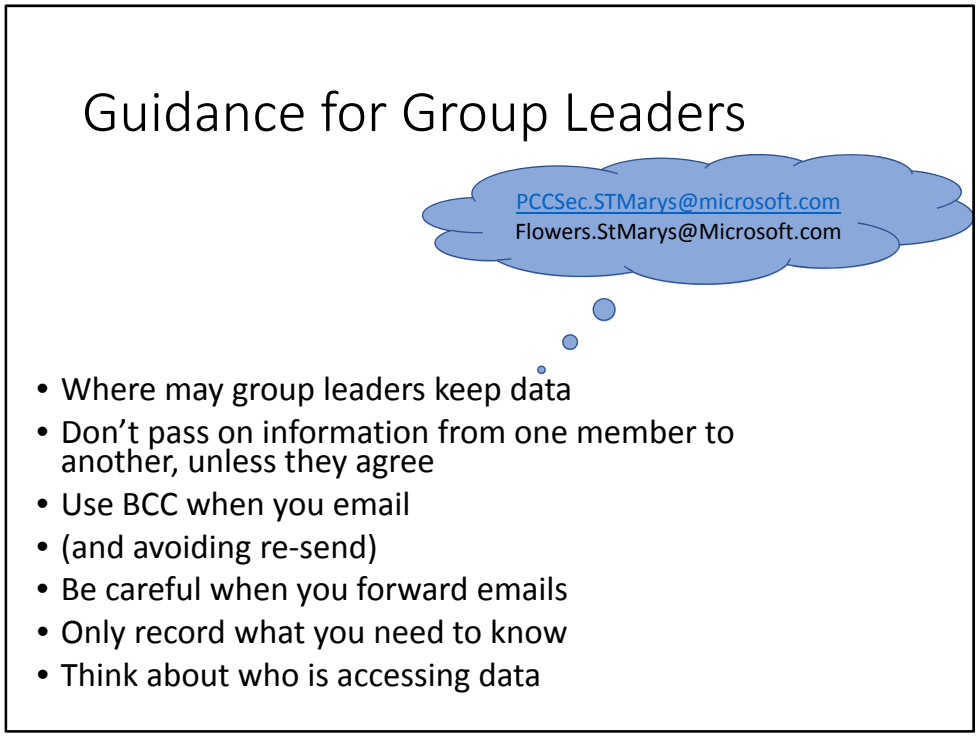
- Children – can consent once 13
- Policy and procedures
  - Data subject requests (sample provided)
  - Data correction
  - Retention (problem is safeguarding)
  - Breach
- Training: who needs to know, awareness
- Security

Children – mentioned above

Policy and Procedures
You need to document various local procedures.

Training
It's not sufficient to have this procedures – who needs to know? How will you make sure everyone following them?

Security
Accident is a bigger risk than maliciousness
Passwords: and password discipline
Locked cabinets



It is the PCC's responsibility to pass this on.

A few things to think about….

Where may group leaders keep data – is there a policy about computers at home, memory sticks, cloud.
[Let the technical people discuss the merits of each, briefly]

Husbands and wives sharing computers (separate logins may be better)
… or email addresses (separate may be better, or even a specific church one. This can be done, even if the church/parish does not have a domain name – see e.g.)

Don't pass on information from one member to another, unless they agree

Use BCC when you email – make sure everyone knows how to do this,

(and avoiding re-send, if the list of names and addresses may have changed in the meantime

Be careful when you forward emails – what addresses are further down the

trail?

Only record what you need to know

Think about who is accessing data

What do we do next?

At the next PCC(4)

- Make sure all consents received.
- Approve procedures, policies
- Make sure everyone who needs to know about them has been informed
- Make sure review dates in forward plan

Make sure all consents received. i.e. programme of back consenting complete
Approve procedures, policies i.e. all decisions made and documented
Make sure everyone who needs to know about them has been informed and everyone is doing this (induction of staff and volunteers)
Make sure review dates in forward plan – don't just leave it – every 3-5 years look through and check that it doesn't need tweaking.