General Data Protection Regulation

Coming into force on 25 May 2018

What is it all about?

- Major update on the 1998 act and originates from the EU
- Controls the way personal data is used by organisations
- Intended to stop organisations misusing your information
- Greater accountability for organisations
- More rights for individuals

How does this affect us?

- We as a church collect and hold personal information
- The PCC is a *Data Controller* – the person or body that determines the purposes and means of processing data
- The clergy are separate Data Controllers – pastoral care contacts

Principles

When we deal with personal data we must…

- Deal with it lawfully, fairly and in a transparent manner
- Collect data for a specific purpose and not use it in other ways
- Ensure the information we have is adequate, relevant and limited to what is necessary
- Ensure inaccurate data is corrected or erased
- Keep it no longer than necessary
- Ensure appropriate security including protection against unlawful processing and accidental loss

Lawful means…

- With consent
- Necessary for performance of a contract
- Necessary to comply with a legal obligation
- In the legitimate interests of the data controller, unless overridden by interests, rights or freedoms of the data subject
- Necessary to protect life
- Necessary to carry out a task in the public interest

Consent means...

- Freely given, specific, informed and an unambiguous indication of wishes.
- Demonstrable – we need proof of consent
- Can be withdrawn at any time
- Opt-in, not opt-out. No pre-ticked boxes
- Not a condition for something else – subscribe to our newsletter to get a free information pack
- Must be clear what consent is for

Special category (sensitive) data

- Racial/ethnic origin
- Political opinions
- Religious or philosophical beliefs
- TU membership
- Genetic/biometric identification
- Health
- Sex life and sexual orientation

Sensitive data requires…

- Explicit consent
- Legitimate interest of a not-for-profit body with a religious aim AND appropriate safeguards AND relates to members, former members and people who have regular contact AND no transfer of information to a third party without consent
- Already made public by the individual
- Necessary for … (list of conditions)

Children

- No special conditions for data relating to children – data protection is not safeguarding
- Children under 13 cannot give consent
- Privacy notices must be clearly understood by the people reading them

Privacy & Electronic Communication Regulations (PECR 2003)

- Delivery of marketing and fundraising communications
- Email & SMS – consent only
- Phone – consent or legitimate interest, specific consent if on TPS
- Post, by hand, etc – OK
- Also about website cookies, but due to be replaced by EU ePR regulations in the near future

Data in the public domain

- Data protection is about how we *use* data regardless of where it came from
- The fact that it is in the public domain does not give us licence to use it as we please. GDPR & PECR still applies

What we need to do

- Data audit – who, what, when, where, how …
- DP policy – internal document to record what we do and why
- Update data collection forms and procedures
- Privacy notice – public document on website to explain what data we hold and why, and the rights of individuals
- Security guidelines – coming soon
- DP contact – email address on website