General Data Protection Regulation (GDPR)

What is GDPR?
- European Regulation effective from 25th May 2018 and most important change to data privacy regulation in 20 years.
- It will protect and empower all EU citizens' data privacy.
- It will reshape the way organizations approach data privacy and use personal data.
- It will harmonise Data Privacy laws across Europe.
- It will give people more rights and protection about how their personal data is used.

Why should we care?
- Each EU state HAS to implement the new regulation - it is the law!
- Fines for non-compliance are staggering, up to 4% of annual turnover or €20 million, whichever is largest.

What is Personal Data?
- Personal data is information about a living individual which is capable of identifying them.

PERSONAL DATA INCLUDES:
- Name (10%)
- Address (10%)
- Date of birth (10%)
- Passport/ID (5%) + EU
data - Information (10%)
- Email (5%)
- Telephone Preference (5%)
- Bank & Debit (10%)
- Credit (10%)
- Sexual Orientation (5%)

The Rules....
- Article 15 grants the 'right of access', requiring the RG to detail what and how personal data is being processed.
- Article 17 grants the 'right to be forgotten', to ensure personal data is deleted when requested.
- Article 20 grants the 'right of portability', to enable individuals to transfer personal data between companies upon request.
- Articles 25 & 32 require companies to implement reasonable data protection measures to protect individuals' data and privacy.
- Articles 33 & 34 require companies to report breaches to supervisory authorities and individuals affected within 72 hours.
- Article 35 requires companies to perform data impact assessments to identify risks, and develop plans to mitigate them.
- Article 37 requires the appointment of a data protection officer to oversee GDPR compliance.

Principles when dealing with personal data:
- Personal data will be processed lawfully, fairly, and transparently.
- Personal data will only be used once an individual has been told what data will be used for.
- Personal data is relevant, adequate, and limited, and stored longer than necessary.

Action!
- Step One: Review all personal data that you hold and, if consent is relied upon, check that it has been obtained correctly.
- Step Two: Review all policies and procedures. Ensure they cover all the rights individuals are entitled to.
- Step Three: Plan how you will access requests for data.
- Step Four: Security - check what security systems are in place to protect personal data. Know what to do if there is a security breach.
- Step Five: Communicate, communicate! Become informed: tell your staff, committees, congregation...

Useful terms
- Processing Data: Anything that is done with/to personal data.
- Data Subject: The individual about whom personal data is being processed.
- Data Controller: Person who determines the how and what of data processing within your parish.
- Data Protection Officer: Person responsible for informing, advising and monitoring compliance within an organisation.
- Consent: Permission must be given to use personal data; and for each use of personal data.

By being GDPR compliant we will:
- Increase openness, transparency, and efficiencies in the way we process individuals' personal data and children's data.
- Be able to respond to requests for information in a timely, organised manner.
- Have robust policies & procedures in place to manage compliance and best practice.
- Maintain trust and give our customers (and community) confidence in how we share and use their personal data.

I want to find out more
- Representative Church Body
- Data Protection Commissioner (Ireland)
- The Information Commissioner (UK)
- European Union

Developed by the Representative Church Body

www.ireland.anglican.org/parish-resources
www.inforights.org.uk
www.ico.org.uk
www.gdprorg