**DATA SECURITY POLICY**

**The Parish of** Enter name of Parish here

1. **Who are we?**

The parish of Enter name of Parish here is the data controller (contact details below).

1. **We hold the following types of personal data:**
* Contact Details
* Family Details
* Financial Information (if provided by you)
* CCTV images
* Photographs
* Etc.
1. **Why do we hold your personal data?**
* For the day to day running of the Parish
* For Contractual Necessity
* To meet our legal obligations
* In the Public Interest
* Etc.
1. **Where do we hold your personal data?**
* On our IT Server
* In the Cloud
* In the Parish Office
* Etc.
1. **What measures have we put in place to keep your data secure?**

The Parish controls access to all personal data by:

* Laptops, USB keys, smart phones and other forms of portable device are especially vulnerable to theft and accidental loss so will always be encrypted
* Updating software and virus protection on all systems, phones, laptops and portable devices
* Passwords on all devices
* Controlling access to personal data on a ‘need to know’ basis only
* Minimising the amount of personal data held by the Parish
* Archiving historical personal data with the RB Library
* Introduction of Pseudonymisation
	+ - **Remote Access:** Where a person processing personal data on behalf of the Parish is authorised to access the network from a remote location (e.g. from home, the Rectory or from an off-site visit) appropriate security measures should be continually assessed. As necessary a Data Privacy Impact Assessment will be undertaken.
		- **Wireless Networks:** As with remote access, wireless networks should be assessed on security grounds rather than solely on their ease of use. Adequate security is in place on the network, e.g. through appropriate encryption measures.
		- **Cloud storage:** is used as appropriate with suitable safeguards in place.
1. **Our Legal Obligations:**

The Data Protection Act (2018) and the General Data Protection Regulations 2016 place an obligation on controllers and processors to implement 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risk.

It suggests the following appropriate measures:

* the pseudonymisation[[1]](#footnote-1) and encryption[[2]](#footnote-2) of personal data
* the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
* the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
* a process for regularly testing, assessing and evaluating the effective of technical and organisational measures for ensuring the security of the processing

The Parish is also obliged to ensure that all those processing personal data on their behalf are aware of security measures and comply with them.

1. **Contact Details:**

If you have any queries on data security, please in the first instance contact the name of parish administrator/contact person at enter the name and contact details of your parish here

You can also contact the Data Protection Commission at: 353 (0761) 104 800 by post at: 21 Fitzwilliam Square South, Dublin 2, D02 RD28 or via email at: info@dataprotection.ie

1. Pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. [↑](#footnote-ref-1)
2. Encryption is the process of encoding information stored on a device and can add a further useful layer of security.  [↑](#footnote-ref-2)