




*RENFREW NORTH
PARISH CHURCH*

GDPR in Renfrew North



What is GDPR?

- The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union.
- The GDPR aims primarily to give control to citizens and residents over their personal data



GDPR Principles

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimalization
- Accuracy
- Storage Limitation
- Integrity & Confidentially
- Accountability

Lawfulness, Fairness and transparency. For data processing to be lawful, we must be able to rely on one of the following legal bases for processing (Condensed list)

- The person has given consent to the processing of their personal data for one or more **Specific Purpose**
- Processing is necessary for the performance of a contract, in with the data subject is part of a binding contract with the church (Church employees)
- Processing is necessary for the legitimate interests perused by the controller or third party.

Purpose Limitation - the data collected must be used for specified and explicit purposes.

*Example: The information collected in the church roll **Can only be used for the specific purpose it was collected for. This can include asking church office staff / roll keeper / office bearer for a member's address.***

Data Minimalization -Only data that is relevant must be stored

*Example: If you keep someone's email address. You **MUST** provide an appropriate reason for holding this, along with evidence that you have used this information before or intend to do in the future*

Accuracy. Every reasonable steps must be taken to ensure the data is accurate and up to date.

Example: Ensuring the congregation is informed how to change their details if there address etc changes.

Storage Limitation – Data collected must only be stored for a reasonable amount of time. Reviews must be taken to decided what information held is still relevant. and required. a data audit should be carried to determine what information is stored, the purpose of the information, the type of information

Example: Information must be deemed relevant to continue to store. For example, not storing members who have left.

Integrity & Confidentiality – Ensuring data remains secure and confidential

Example: Ensure security systems are in place – Either Physical (Lock & Key) or digitally (Encryption / Password protection)

Accountability- The data controller must be able to demonstrate compliance with the first 6 principles.



Personal Information

Personal Information Is Defined as:

Staff/payroll records; membership lists; baptismal records; information relating to pastoral care; information regarding those attending holiday clubs or other activities; lists of children/young people attending Sunday schools, youth groups and creches; records of those for whom the congregation holds contact details for various reasons, including volunteers working with children and young people and others, those attending churches, making Gift Aid donations etc.

What is personal data?' Up on the screen now is the definition of personal information provided by 121. As you can see, these laws now require that all of this information is stored safely and securely.



Who is Affected?

- **Office Bearers** with access to Personal Information
 - Minister, Session Clerk, Clerk to the Board, Treasurer, Property, Finance, FWO, Hall lets, Roll Keeper, Office Staff,
- **Church Organisations** that are governed by the Church
 - Junior Church, Guild, Mens' Association, Coffee Bar, Pipe Band, Christian Aid Group, Prayer Group
- **Elders with District Responsibilities**
- **Church Employees**

What does this mean for Renfrew North?



- Office bearers that handle sensitive information **must now use the church email system for communications** (@renfrewnorth or @churchofscotland Email addresses)
- Database Systems that hold sensitive information, Including the church roll system, **must be assessed for relevance and moved to a central system stored within the church systems**
- Information stored by church organisations, e.g. consent forms **must be stored securely either digitally, or physically secure.**

So by this point you must be thinking, 'how this affects us'

The three main things we need to change are up on the screen.

Firstly, office bearers that deal with confidential information, this includes, personal, financial or confidential must use the church managed email system for the primary point of communication. Using personal email accounts provide a would be attacker an easy way to access confidential information.

Secondly, and probably one of the biggest ones is changes to the roll system. Currently the roll system is stored by Sandra, and changes are distributed monthly. There system is very prone to attack and we can now be prosecuted if this information is lost or stolen. The proposed change is to move all data onto the church managed system. The system we employ is designed by ourselves, which allows us for large control over the use of the system, whilst still allowing external users such as the minister to access the data. This would also provide a benefit for workflow, as there will be one central copy of the roll, as opposed to multiple copies held by multiple people.

The final recommendation is to ensure that information stored by organizations are kept secure. It is the responsibility of the church to ensure that organisations are also compliant with the new regulations. This includes organizations who share cupboards.



Next Steps

- Appoint a Data Protection Officer (DPO)
- Meeting with Key office bearers
- Meeting with Organisation Representatives
- Ensure data subjects are informed of their rights, and implement a policy for all GDPR related requests

So, what's next?

The first key step is to appoint a Data protection officer. It is a requirement that each congregation has a DPO to to advise on compliance, conduct information audits and provide appropriate training and support.

The next step would be to have two preliminary meetings, firstly with Office bearers to gain a picture on what information they store, why they store it and how they store it. This meeting would also be an appropriate time to provide support to move users on to the church managed email system. A meeting with a representative from each organization would also be beneficial, as again, we need to know, what, how and why they store confidential information.

The final point is to properly inform data subjects (Congregation) on their new rights under the GDPR. We are required to provide a notice in a public place informing of the relevant rights, this has been prepared with guidance from 121



*RENFREW NORTH
PARISH CHURCH*

GDPR in Renfrew North

Questions?