

DATA PROTECTION AND GDPR FOR PARISHES A QUICK GUIDE



What is the GDPR?

The General Data Protection Regulation is a regulation in EU law which standardises how data can be processed, giving people more control over their data. It is intended to make it easier to understand how data is being used.

Following Brexit, this still applies to the UK and a revision of the GDPR, known as the 'UK GDPR' will come into force in 2021.

The Data Protection Act 2018 sets out the framework for data protection law in the UK. It sits alongside the GDPR and tailors how it applies. The regulatory body in the UK is the Information Commissioner's Office (ICO).

'Processing'
refers to any
collection, storing,
sharing, deletion,
updating and
other uses of
personal data.

The 'Data
Controller' is the
person or
organisation who
determines the
how and what of
data processing.

How does it affect the Diocese?

The GDPR applies to all organisations that process personal data of EU citizens including the Diocese of Hexham and Newcastle.

As the data controller and owners of Diocesan data, the trustees/directors of the Diocese have the overall responsibility of ensuring compliance for the Diocese including partnerships and parishes.

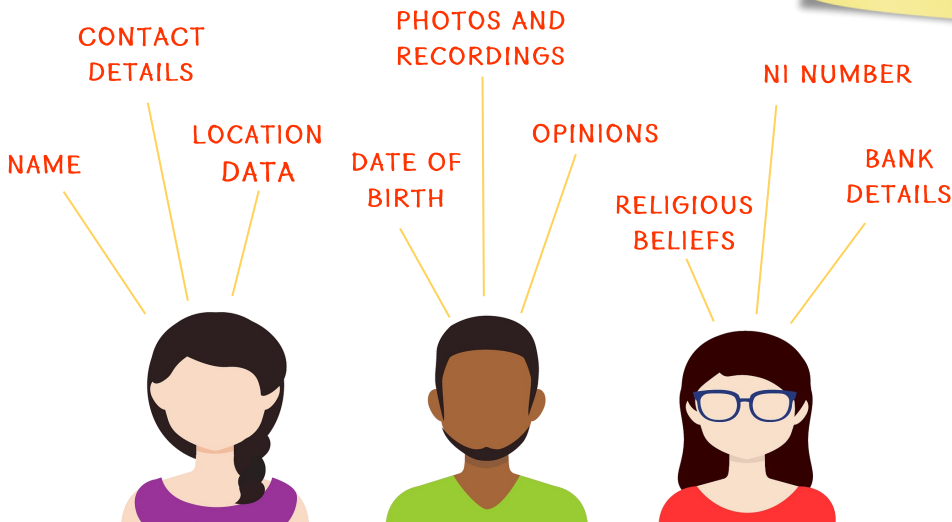
Who needs to comply?

All clergy, employees, religious and volunteers in the Diocese have a duty to comply with the GDPR and data protection regulations. The Diocese has a Data Protection Team to provide information, support, policies and procedures relating to data protection to assist with compliance.

What is Personal Data?

Personal data is any information relating to a living individual, or *data subject*, who can be identified directly or indirectly from that data. Examples are given below:

The 'Data Subject' is the person about whom data is processed.



Data subjects include parishioners, clergy, children, volunteers, contractors, visitors to the parish and employees.

Special Category Data is highly sensitive data relating to or about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, or sexuality.

Personal data can reveal a great deal about people and therefore it is vital we treat this data with respect and ensure it is processed appropriately.

Why do we process personal data?

There are many reasons why parishes and partnerships may need to process personal information, including:

- allowing the parish priest to keep in contact with parishioners
- contacting parish volunteers about their roles
- keeping a diary of appointments
- Sacramental preparation and recording of this, e.g. baptism or marriage applications and registers
- keeping track of parish finances and planned giving
- hiring out facilities
- facilitating parish clubs and events
- carrying out safeguarding checks for volunteers
- records of children's liturgy attendance for safeguarding purposes
- operating a CCTV system
- putting together the parish newsletter

...AND MANY MORE

Processing Personal Data lawfully

Whenever personal data is processed, there must be a lawful basis for doing so.


Legitimate Interest

We can often rely on it being in the legitimate interest of the parish/partnership to process data, i.e. there is a purpose identified and it is necessary to process personal data to achieve this.

Examples include:

- collecting information in relation to baptisms or marriages
- keeping contact details of volunteers to contact them about their role
- having a CCTV system in or outside of the church/presbytery.

Without processing this, the parish would not be able to perform in its duties and achieve its purpose. This is appropriate when personal data is used in a way that people would **reasonably expect**, it has **minimal impact on their privacy** and will not **cause harm**.



Please be aware that there is a difference between requiring people to consent to something and using consent as a basis for processing data. For example, you may use a parental consent form when planning an activity with children. However, you would not rely on consent as the basis for collecting and storing the information on the form. Legitimate interest would be more appropriate as without the information, the parish could not facilitate the activity and withdrawing consent would mean the person could not take part.

Consent

Usually consent is used when you wish to either share people's personal information with others or where you would like to send people information electronically that can be classed as 'marketing'. For example:

- passing on contact details of rota volunteers to other volunteers
- publishing names of those who are sick in a parish newsletter
- providing Eucharistic Ministers with details to be able to visit a parishioner
- emailing information about parish events to parishioners

Consent is used when you can give people **choice and control** about the use of their personal data and they have the **option to withdraw or change** that consent, e.g.

- someone who previously signed up to receive emails about events may choose not to receive them anymore
- someone requesting their name is removed from the published sick list

Consent must be **freely given** and requires a **positive opt-in**. It must be very clear what is being agreed to. When you obtain consent, you must keep evidence of this. If consent is given verbally, a record needs to be kept.

Template forms on the Diocesan data protection webpage provide examples of the use of consent and an example of a verbal consent record.

Processing Personal Data lawfully cont.

Contract

A contract may be used where you provide someone with a service, e.g. the hire of a facility.

Legal Obligation

When processing personal data for the purposes of complying with law or a statutory obligation, legal obligation is the lawful basis. This could be when collecting data to process Disclosure and Barring Service checks for volunteers or when information is passed to the Diocese or HMRC to process Gift Aid donations.

Vital Interests

This would be the basis when you need to process the data to protect someone's life, e.g. passing information about an individual's serious health condition to the NHS.

Public Task

This is usually used when processing is carried out in the exercise of official authority, e.g. updating the civil register of marriages.

What rights do data subjects have?

Every data subject has rights when it comes to the processing of personal data.

The right to be informed

We must let people know how and why we use their data. This is achieved by using privacy notices when collecting information.

The right of access

Data subjects can submit a subject access request to obtain access to data that the parish or Diocese holds about them. See *further information on this overleaf*.

The right to rectification

Data subjects can request that data held about them is corrected to ensure it is factual and up to date.

The right to restrict processing


Data subjects, in certain circumstances, may request that any processing of their personal data ceases. This means the data is still stored but cannot be used.

The right to erasure

Data subjects can request that their personal data is no longer processed and should be erased. Where possible and appropriate, this should be adhered to.

The right to object

Data subjects can object to the processing of their data, e.g. they may withdraw a previous consent.

 Not all rights are absolute in every circumstance so if you are unsure if you have to comply with a request, please contact the Data Protection Team (DPT). When dealing with the rights to access, rectification, erasure and objection, the Diocese has one month to respond from the time of the request. Parishes must contact the DPT immediately so this timescale can be met.

Personal Data Breaches

What is a personal data breach?

A personal data breach is defined in the GDPR as:

"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

Examples of a breach are as follows:

- the disclosure of confidential data to unauthorised individuals, e.g. an email containing personal data is sent to the wrong group of people
- the loss or theft of records, e.g. a batch of hardcopy records containing personal data is lost or stolen
- the loss or theft of devices or equipment that may contain personal data, e.g. a USB device containing personal data is lost or stolen
- a suspected breach of IT security that could have allowed unauthorised access to personal data, e.g. an unknown third party has gained access to a parish computer
- a breach of physical security e.g. forcing of a door or window to gain access to a secure room.



What should we do if we think there has been a breach of personal data?

The person who has identified the possible breach must contact the Data Protection Lead (DPL) **immediately**, preferably by telephone on 0191 2433300.

Subject Access Requests

Any person may exercise their rights to access and request to find out what data the Diocese holds about them, or the right to have their data modified or erased.

Any such requests should immediately be referred to the DPL using the contact details in this booklet.

A request will most likely come in writing by email or letter. If you receive a verbal request, ask the person to put it in writing or use the form on the Diocesan data protection webpage at www.rcdhn.org.uk/dataprotection/dataprotection.php

There is a strict timescale to deal with these requests imposed by the ICO. If you are not sure if a request would qualify as a subject access request please contact the Data Protection Team.

General Data Security

- ✓ **DO** minimise who has access to personal data. Decide if people who currently have access really need to. This may mean storing data for different purposes in separate areas.
- ✓ **DO** ensure key holders for parish properties are kept to a minimum. Number the keys and keep records of who has them. If they no longer need access, make sure these keys are returned.
- ✓ **DO** work on the basis of 'a box within a box' for security, e.g. records stored in a locked cabinet which is inside a locked office or a password protected document on a password protected computer.
- ✓ **DO** lock all portable devices away when not in use.
- ✓ **DO** have a clear desk policy for when people are not at their workstation.
- ✓ **DO**, where possible, store parish data at the parish. Staff and volunteers may need to transport data offsite but data kept offsite from the parish must only be the minimum required. This should be returned to the parish as soon as possible.
- ✓ **DO** ensure you know exactly what information your volunteers hold/transport if they are required to take data offsite.
- ✓ **DO** ensure that when personal data is removed from an office, it is subject to appropriate security measures, including keeping paper files away from public visibility, making sure nothing is left in vehicles and ensuring it is stored securely in homes.
- ✗ **DON'T** display personal data in offices that may be used by volunteers or to receive visitors.
- ✗ **DON'T** leave visitors unsupervised in offices where data is not secured.
- ✓ **DO** ensure that when getting rid of personal data, paper documents are securely shredded and electronic data deleted securely (make sure data is deleted from the Recycle Bin folder on your computer).



Information Technology Security

- ✓ **DO** use individual logins and passwords for computers and other devices and don't share these.
- ✓ **DO** use complex passwords (using both upper and lower case letters and including numbers and special characters) or pass phrases. Passwords should be changed regularly and when there is a change in personnel.
- ✓ **DO** restrict access to the parish email account to only those who absolutely need it. A person emailing the parish would have a reasonable expectation of confidentiality.
- ✗ **DON'T** use a personal email address for sending personal data if others have access to this, e.g. a family email account.
- ✓ **DO** keep files organised in a system of folders and not saved to the desktop.
- ✓ **DO** password protect documents containing sensitive personal data. If sharing a password protected document by email, communicate the password via another method, e.g. by text message or over the phone.
- ✓ **DO** log off your computer or lock your screen when working away from your device.
- ✓ **DO** position computer screens away from windows and walkways to prevent accidental exposure of personal data.
- ✓ **DO** install anti-virus software and malware protection on all computers used to process personal data. Anti-spam protection should be used for emails.
- ✓ **DO** back up information stored on parish computers regularly. This can be to an external hard drive, a password protected USB device or to a cloud service.
- ✓ **DO** delete out of date back-ups of information.
- ✓ **DO** use password protected storage media, i.e. USB devices or external hard drives. Many USB devices have software included to be able to add encryption. These devices should be locked away when not in use.
- ✗ **DON'T** allow any unknown third party to have remote access to a computer unless you have requested this.
- ✓ **DO** be aware that if you are using a Wi-Fi connection on a device that contains personal data in a public place, you must not link to any public access network.



Consequences of non-compliance

The consequences of non-compliance can be severe. In addition to the risk of lawsuits from breach victims, disruption to business and damage to the reputation of the Diocese, the ICO can now impose fines of up to £20,000,000 or 4% of annual turnover. Although unlikely that such harsh fines would be issued, it is vital that we make all efforts to protect personal data to avoid any negative outcomes.

Support for parishes

Diocesan Website

The Diocese has a dedicated webpage for data protection support which includes policies, guidelines and example forms. This can be found at:
www.rcdhn.org.uk/dataprotection/dataprotection.php

Data Protection Team

The following members of curial staff provide support for parishes in relation to data protection and GDPR:

Data Protection Lead (DPL)	Data Protection Support Manager (DPSM)	Head of Human Resources
Jeff Ledger	Catherine Joyce	Katherine Nugent
0191 2433300	0191 2433317	0191 2433301
Point of contact for data breach or subject access reporting	Point of contact for general enquiries	Point of contact for enquiries relating to employees or volunteers

To contact the team by email, please send queries to
data.protection@diocesehn.org.uk

If you need any information or support, please do not hesitate to get in touch with us. We will be happy to help you.