GAP

Guidance, Advice and Practice

Paper 14 Data Protection and Child Safeguarding

THE NATIONAL BOARD FOR
SAFEGUARDING CHILDREN
IN THE CATHOLIC CHURCH IN IRELAND

About the GAP Paper

The National Board for Safeguarding Children in the Catholic Church in Ireland (NBSCCCI) was established to provide advice, services and assistance in furtherance of the development of the safeguarding of children within the Roman Catholic Church on the island of Ireland. The NBSCCCI also monitors compliance with legislation, policy and best practice and reports on these activities annually, as comprehensively set out in the Memorandum of Association of the Company, Coimirce.

Article 4 (iii) of the Memorandum and Articles of Association of the Company requires the NBSCCCI to: report and provide, upon request from the Constituents or any Constituent, support, advisory and training services to such Constituents or Constituent on policies and practices relating to safeguarding of children.

The NBSCCCI already provides comprehensive Guidance to support the implementation of *'A Safe and Welcoming Church: Safeguarding Children Policy for the Catholic Church in Ireland 2024'*. These series of Guidance, Advice and Practice (GAP) papers further complement the detailed guidance on topics of current interest to constituents.

A major part of quality assurance, which is the responsibility of the Church authority, is becoming aware of new challenges or gaps to safeguarding as they emerge. This series of papers aims to provide the reader with information on guidance, advice and practice, which will assist in developing best practice in safeguarding children, identifying where there are risks and how to minimise these risks. To do this, these papers draw on the experiences of the NBSCCCI, research and information already available to the reader from other sources.

The GAP papers are not intended to be read as definitive positions on the chosen topic. The NBSCCCI does not claim to have inserted all available research and knowledge; nor do we claim to be masters of best practice, offering indisputable views. Each of these papers will focus on a particular gap in terms of safeguarding children, and each paper will provide guidance, advice and practice to help overcome these gaps, building the reader's knowledge on the subject and in informing practice, which will be underpinned by the safeguarding standards, Leadership Governance and Accountability, Nurturing a Culture of Safeguarding and Responding Pastorally according to Civil and Canon Law.

Specifically, this paper has been written to gather research and information to guide the Church on building its data protection policies in line with data protection legislation.

Contents

Terminology	page 3
1. Introduction	page 4
2. Data Protection	page 5
3. Background & Legislation	page 6
4. Key Stakeholders	page 7
5. Data Storage	page 8
6. Data Retention	page 9
7. Civil & Canon Legal Rationale for Data Retention	page 11
8. Data Breach & Data Access	page 13
9. Data Destruction	page 14
10. Conclusion	page 15
References	page 16
Appendix 1: Sample Retention Schedule of Safeguarding Documents	page 17

Terminology

Set out below are terms used throughout this document, accompanied by an explanation to aid the reader.

Data controller: the organisation deciding how to use the data.
Data processor: the organisation processing the data on behalf of the controller.
Data subject: the individual the data relates to.
DPIA: Data Protection Impact Assessment -The process by which risks are identified, and the impact of those risks is determined.[1.]
DPC: Data Protection Commission. Ireland's independent authority is responsible for enforcing data protection laws and protecting individuals' data privacy rights.
GDPR: General Data Protection Regulation.
Indirect personal data: Information which identifies a person when combined with other data including IP address, location history, employee number, online usernames and device indicators. Reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person can identify an individual or make them identifiable. [2.]
ICO: The Information Commissioner's Office is the UK-wide authority responsible for upholding information rights with a regional office in Belfast that serves as a local point of contact in Northern Ireland.
Personal Data: Information relating to an identified or identifiable individual. This includes obvious identifiers like names and addresses, but also online identifiers like IP addresses and location data.
Personal data breach: is 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.
PIA: Privacy Impact Assessment, a systematic process used to identify, assess, and mitigate the privacy risks associated with new projects, systems, or processes that involve the collection, use, or disclosure of personal information. [3.]
Processing: Any operation performed on personal data, such as collection, recording, storage, use, and disclosure.
Special categories of personal data (sometimes referred to as "sensitive personal data") are types of personal data which are subject to stricter processing requirements. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Legitimate interests [4.] is a versatile and flexible legal basis for the processing of personal data, which may apply in circumstances where processing operations do not fit neatly into any of the other legal bases; however, it also carries heightened obligations on controllers to balance the legitimate interests they are seeking to pursue with the rights and interests of the data subject.

1. Introduction

As part of its work, the National Board for Safeguarding Children in the Catholic Church in Ireland (NBSCCCI) staff engage with Church authorities to provide advice and guidance on safeguarding matters.

The EU General Data Protection Regulation (GDPR)[5], the Data Protection Act 2018 [6.] in the South, and UK GDPR and Data Protection Act 2018 [7], in the North govern data protection in all organisations on the island of Ireland, including the Catholic Church.

Policies on data protection should be structured at both diocesan and parish levels for dioceses and at provincial and community level for religious congregations, with specific guidelines for sacramental records and safeguarding. The Church, like any other body, is required to handle personal data lawfully, fairly, and transparently, and to ensure data is securely maintained.

Data protection and safeguarding within the Church intersect in complex ways, requiring careful alignment between data protection principles and safeguarding obligations, particularly where information relating to abuse allegations must be shared to protect children.

This paper aims to:

1. **H**ighlight data protection principles.
2. **E**xplore the roles, rights and responsibilities of stakeholders.
3. **D**emonstrate best practice for Church authorities identifying which data protection policies and procedures should be in place within each body.
4. **F**ocus on the legislation frameworks, both north and south, demonstrating how to be compliant
5. **P**rovide examples of civil and canon law justifications for the storage and retention of some key data.

Storage and retention of data is often an area of confusion within data protection; a desire to retain information as proof of an action may, at times, contravene data protection principles. It is the aim of this GAP Paper to provide guidance on this topic (Appendix 1) and provide guidance on managing risks such as this.

2. DATA PROTECTION

Data protection is defined as the legal and technical framework used to safeguard the privacy rights of individuals by controlling how their personal information is collected, processed, and stored.

While definitions vary slightly by jurisdiction, they generally centre on two main pillars:

- **Legal Privacy Rights**: Ensuring personal data is used fairly, lawfully, and transparently, giving individuals (data subjects) control over their information.
- **Technical Security**: Implementing strategies and processes—such as encryption, backups, and access controls—to protect data from corruption, loss, or unauthorized access.

Personal data is any information that can identify a living individual, either directly or indirectly. Different pieces of information, which, collected together, can lead to the identification of a particular person, also constitute personal data.

Direct personal data that identifies a person on its own includes full name, passport or national identification number, email address.

Indirect personal data which identifies a person when combined with other data includes IP address, location history, employee number, online usernames and device indicators. Reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person can identify an individual or make them identifiable.

In practice, any data about a living person who can be identified from the data available (or potentially available) will count as personal data. This will include pseudo-nominised data i.e. replacing any identifying characteristics of data with a value which does not allow the data subject to be directly identified (pseudonym). Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data.

Data protection is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights. Legal frameworks in both the north and south are designed to give individuals control over their personal information.

Organisations must follow six core principles when processing data:

- **Lawfulness, Fairness, and Transparency:** Data must be processed legally and openly.
- **Purpose Limitation:** Data should only be collected for specified, explicit, and legitimate purposes.
- **Data Minimisation:** Only collect data that is strictly necessary.
- **Accuracy:** Keep data up to date and correct errors.
- **Storage Limitation:** Keep data only for as long as it is needed.
- **Integrity and Confidentiality:** Ensure data is secured against unauthorized access or loss.

Key Individual Rights under GDPR
Under GDPR, individuals have specific rights regarding their personal data:

- **Right of Access:** An Individual can request a copy of the personal data held about them.
- **Right to Erasure ("Right to be Forgotten"):** An Individual can request that their data be deleted when it is no longer necessary or if they withdraw consent.
- **Right to Rectification:** Individuals have the right to have inaccurate or incomplete data corrected.
- **Right to Data Portability:** Individuals can receive their data in a machine-readable format to transfer it to another service.
- **Right to Object:** Individuals can object to their data being processed for direct marketing or based on their specific situation.

Data Protection vs. Data Privacy: Privacy is about *who* has authorized access to data and how it is shared, whereas protection is the broader set of *tools and policies* (including security) used to enforce those privacy rules.
Scope: Data protection laws generally apply only to personal data relating to a living individual.

Fully anonymised data that cannot be linked back to a person typically falls outside the scope of these regulation.

3. Background and Legislation

GDPR (2018): The General Data Protection Regulation (GDPR)[7]. was adopted in 2016 by the EU and became enforceable on May 25, 2018. Unlike the previous Directive, it is a Regulation, meaning it applies directly across all EU member states without needing national implementing laws, ensuring a uniform standard.

The management of data in Ireland, north and south, is primarily governed by the EU's GDPR (General Data Protection Regulation) and the national Data Protection Act 2018,[8]. enforced by the Data Protection Commission (DPC) in the south and the UK GDPR Data Protection Act 2018, enforced by the ICO in the North. Key principles include lawful, fair, and transparent processing, data minimisation, and security, granting individuals rights like access, correction, erasure, and portability, while imposing obligations on organisations (controllers/processors) to safeguard personal data with appropriate measures.

Beyond avoiding significant fines from regulatory bodies like the https://www.dataprotection.ie/en proper data protection fosters trust within the community. It prevents potential harm—such as identity theft or emotional distress—that could arise from a data breach.

Earlier data protection principles had been established in 1995, prior to smartphones, social media and cloud storage. This ever-evolving world of technology requires a strong regulatory framework.

Data protection in the church is a legal and moral obligation to safeguard the personal information of congregants, staff, volunteers, victims and survivors of abuse priests and religious, As "people protection," it ensures that sensitive data—such as sacramental records, prayer requests, allegations of abuse—is handled with the respect and dignity it deserves.

Key Legislation

- **General Data Protection Regulation (GDPR):** Directly applicable since 2018, this EU-wide law sets high standards for how organizations handle "personal data"—any information that can identify a living person.
- **Data Protection Act 2018** is the national legislation that gives further effect to the GDPR and transposes the Law Enforcement Directive (LED) into Irish law.
- **ePrivacy Regulations (2011)[9].:** Rules specifically for electronic communications, including cookies, direct marketing (email/SMS), and location data.
- **UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018**[10]. These laws govern how personal information is used, mandating lawful processing, accuracy, security, and specific rights for individuals regarding their data.
- **UK GDPR:** Governs within NI the processing of personal data, focusing on principles like lawfulness, fairness, transparency, and accountability.
- **Data Protection Act 2018:** Complements the UK GDPR, covering in NI areas such as law enforcement and general data processing.

The Regulatory Specifics in Ireland

- **Digital Age of Consent:** Set at 16 years old in Ireland. Children under 16 require parental or guardian consent for online services.
- **Enforcement:** The DPC has the power to conduct audits, issue enforcement notices, and impose substantial administrative fines (up to €20 million or 4% of global turnover).
- **Breach Reporting:** Data controllers must notify the DPC of a data breach within 72 hours if it poses a risk to individuals.
- **CCTV and Monitoring:** Use must be proportionate and justified by a clear purpose (e.g., security), with prominent signage required.

The Regulatory Specifics in Northern Ireland

- **Privacy and Electronic Communications Regulations**[11]. (PECR): These govern electronic marketing (emails, SMS), cookies, and telecommunications privacy.
- **Freedom of Information Act 2000 (FOIA)**[12].**:** While distinct, it often overlaps with data protection regarding Subject Access Requests (SARs) and the public's right to access information held by public authorities in NI.

4. Key Stakeholders

Data Controller
Under General Data Protection Regulation (GDPR) and similar privacy laws, organisations are categorised as either data controllers or data processors based on their level of decision-making power over personal data.

A data controller is the individual or the legal person who determines the purposes and means of the processing of personal data; in other words, the controller makes material decisions relating to the processing of personal data, such as determining the purposes for which personal data is collected, stored, used, altered and disclosed. As a result, most of the responsibilities for General Data Protection Regulation (GDPR) compliance rest with the data controller, such as providing information to data subjects, ensuring there is a legitimate basis for processing activities, giving effect to data subjects' rights under the GDPR, and ensuring that there is appropriate security for data processed.

Within Church bodies in Ireland the Data Controller holds overall responsibility for ensuring compliance with data protection legislation. The Data Controller determines:

- The purposes for which personal data is collected and processed by safeguarding personnel.
- The means and manner by which safeguarding personnel process personal data in the course of their duties

A data subject would normally be entitled to transparency about the processing of their personal data. However, that information may be withheld or delayed where notifying the individual would prejudice an ongoing Garda/PSNI investigation, child-protection inquiry, criminal process, or related safeguarding investigation. (ROI Data Protection Act 2018 s94(2)(a)&(b) & UK Data Protection Act 2018 Schedule 2, Part 1, Paragraph 2).

DATA PROTECTION OFFICER (DPO)
Some data controllers are required to have a Data Protection Officer (DPO) and others choose to have a DPO (or an assigned individual) to deal with data protection matters on their behalf. The DPO can also be contacted by individuals if they have data protection queries or concerns.
If there is no DPO in a company, other people in the company will then address any data protection queries or concerns on behalf of the data controller.

It is important to note that those individuals within the organisation are not data controller themselves; they are simply acting on behalf of the data controller.

DATA PROCESSOR
A data processor is the individual (other than an employee of the controller) or the legal person that carries out processing activities, on behalf of and in accordance with the controller's instructions. In other words, the data controller can provide personal data to the data processor to carry out such processing activities on its behalf. A data controller does not need the consent of data subjects to engage a processor. Arrangements between the data controller and data processor are governed by a legal agreement. Any queries an individual may have regarding the role of the processor ought to be directed back to the data controller who engaged the processor in the first place. For example, NBSCCCI independent reviewers are data processors during safeguarding reviews of Church bodies.

DATA SUBJECTS
People have a right to know what personal information is held about them, by whom and for what purpose. This is detailed in data protection and human rights legislation. However, despite these rights, in certain circumstances such information can be shared with others.

CHILDREN
General Data Protection Regulation (GDPR), which became applicable as a law on 25 May 2018, recognised for the first time in EU data protection law the specific circumstances and risks posed to children when their personal data is collected and processed without adequate safeguards. GDPR emphasises the need for clear communication with children around how their personal data is processed when services are being targeted at them and points out that children may be less aware of the risks involved. In addition, it recognises the right of children to exercise their data protection rights, for example to have their personal data erased by online services so that they are not burdened in adulthood with decisions they made around their personal data when they had less understanding of the consequences of sharing their data in the digital environment. (DPC December 2021)

Core Definitions
Data Controller: The entity that determines the **"why"** and **"how"** of data processing. They decide what data to collect, for what purpose, and how long to keep it.

Data Processor: The entity that processes personal data **only on behalf** of the controller and follows their specific instructions. They do not own or have independent control over the data.

5. Data Storage

Data storage safety across the island of Ireland is governed by strict GDPR regulations requiring appropriate technical and organisational measures to ensure confidentiality, integrity, and availability

Key obligations include encryption, secure physical storage (locked cabinets), access control, regular backups, and mandatory data retention policies.

- **Security Measures:** Data must be protected against unauthorised access, alteration, disclosure, or destruction. This includes using anonymisation, encryption, and secure backups.
- **Physical Security:** Manual files must be kept in locked cabinets or rooms with restricted access.
- **Retention:** Data must not be kept longer than necessary for its intended purpose.
- **Staff Training:** Employees must be trained on data security risks, and access permissions should be removed quickly for staff leaving an organisation.
- **Breach Management:** Strict reporting protocols are required if data is lost or stolen.

Best Practices

- **Risk Assessment:** Security measures should be appropriate to the risk, considering the "state of the art" and implementation costs.
- **Portable Devices:** Laptops, USB sticks, and tablets must be encrypted and securely stored when not in use.
- **Accountability:** Organisations must be able to demonstrate compliance with these principles

It is important that all sensitive or confidential materials in relation to a safeguarding case are retained in a case file and stored securely in a place designated by the data controller, i.e. the bishop or superior. Files containing sensitive or confidential data should be locked away, and access to the relevant fireproof safe(s) or filing cabinet(s) and keys should be strictly controlled.

Access to the case management files needs to be limited to people in named roles i.e. the bishop or superior, and properly designated child safeguarding personnel, who either need to know about the information in those records /or who have a responsibility to manage the records.

Any information of a sensitive and confidential nature, if stored electronically, must always be password-protected.

Arrangements need to be made for the contents of the relevant files, as well as their location and storage arrangements, to be passed on by outgoing data controllers to their successors.

Other records with identifying personal information e.g. parish records on recruitment and vetting, activity attendance records, consent forms, accident forms, etc. must be stored in a secure locked cabinet in the parish office.

6. Data Retention

Both jurisdictions in the island of Ireland apply the **GDPR principle of storage limitation,**[14], requiring data to be kept for "no longer than is necessary" for the purposes for which it was collected. Specific retention periods for business, tax, and employment records are largely dictated by local supporting legislation, which results in slightly different timeframes between the two jurisdictions.

The precise rules can vary. Data retention best practices involve establishing a formal policy that minimises risk by keeping data only as long as necessary for legal, regulatory, or business needs. Key actions include classifying data, automating destruction schedules, ensuring secure storage, conducting regular audits, and training staff to maintain compliance with regulations like GDPR.

Determining an appropriate retention period for other documents typically involves considering how long the document remains useful and balancing that utility against the associated cost and risk of storage.

Why have a records retention schedule?

- Records are kept or destroyed consistently, rather than relying on the best guess of staff.
- Records are kept for as long as necessary to meet statutory, regulatory and business requirements
- Resources are not wasted on storing records longer than necessary.
- Any risks arising from holding documents and information are managed.
- The organisation can confidently account for which records are no longer held (for example, in response to a Subject Access Request).
- Staff working with records understand their responsibilities and are given clear information about when and how to destroy records.

Retention Policies and protocols can be established in line with guidance from the relevant data protection authority: the Information Commissioner's Office (ICO) in Northern Ireland or the Data Protection Commission (DPC) in the Republic of Ireland.

Guidance published by the DPC, in relation to compliance with the Data Protection Acts 1998–2003[15], is a useful reference for organisations to consider, as it represents what can be regarded as best practice. This guidance states, inter alia, that:

> ***Where there is no legal requirement to retain information beyond the closure of the record, the authority will need to establish its own retention periods***

All organisations are required to adhere to the Record Retention guidelines to ensure that:

- Legal and regulatory requirements are met. Some laws specify maximum and minimum retention periods.
- The organisation can provide evidence when needed. Proper retention ensures records are available to data subject requests, support audits, investigations, disputes or historical reference.
- **Personal data is not kept longer than necessary**. This helps protect individuals' privacy and prevents unlawful processing of data.
- **Information is well managed and accessible**. Clear retention rules support efficient information management, ensuring personnel know what to keep, where and for how long
- **Storage costs and risks are controlled**. Retaining information longer than needed increases storage costs, cybersecurity exposure and the risk of data breaches.
- **Old or duplicate records are disposed of safely**. Proper disposal reduces clutter, avoids confusion and ensures sensitive information is destroyed securely. Records are retained or destroyed consistently.

This is just as important for digital records as for paper.

There are generally three procedures to follow with regards to the disposal of your records once they have reached the end of their recommended retention period:

• Confidential Destruction: If the records are no longer required for business purposes and have been retained for the recommended retention period, in line with any legislative or statutory obligations, they should be confidentially destroyed/deleted, in line with the Disposal action listed in the Schedule.

• Archival Value: All records that are of potential historical value should be transferred for permanent preservation once their administrative use is concluded.

• Retain for Operational Purposes: In some cases, records will need to be retained for long-term operational purposes. Owners of the records should ensure that these remain accessible for as long as required and are managed appropriately throughout their lifecycle.

IMPORTANT NOTES FOR CONSIDERATION

If you only have a convenience/working copy of a document, and did not create or have responsibility for it, then you may destroy it as soon as you no longer require it for administrative purposes.

If litigation is ongoing, some records may need to be retained for longer than is specified within the schedule to support any litigation process.

Furthermore, if records are subject to a current Data Protection request, they must be retained for 40 days after the request has been fulfilled.

Canon Law and Retention.

Canon Law requires the retention of specific sacramental and administrative records for the Church's operation, while mandating the destruction of certain confidential, moral-related files after specific periods.

- Archival and Permanent Records: Canonical records such as baptismal, marriage, and death records are considered of historical importance and are generally kept indefinitely.
- Confidential Files: Personnel and other sensitive files are considered private, and information should be kept no longer than necessary.

Civil Law Compliance (GDPR): While Canon Law dictates internal procedures, it does not overwrite civil data protection laws (such as GDPR in Europe), which require the Church to have a legal basis to retain personal data.

Rights and Conflicts

- **Right of Access:** Under both Canon 487 §2[16] and GDPR, individuals have a right to access public documents pertaining to their own status (like baptismal certificates) and their own personnel files to ensure accuracy.
- **Right to Erasure:** While GDPR generally grants a "right to be forgotten," this can be limited in a religious context. For example, in 2023 the Irish Data Protection Commissioner ruled that people do not have the right to erasure of their baptismal record under GDPR. Rather the Church has a lawful basis to keep sacramental records for legitimate interests (Article 6 GDPR). The remedy here is annotation, not erasure.

7. Civil and Canon Legal RATIONALE for Retention

Legislative/ Statutory Regulations	Canon Law Instrument
Legislative/ Statutory Regulations	**Canon Law Statutes**
ROI: Criminal Justice (Withholding of Information on offences against Children and Vulnerable Persons) Act 2012 **NI:** Under Section 5 of the Criminal Law Act (NI) 1967, it is an offence to fail to report a "relevant offence" (generally an arrestable offence) if you have information that could help secure a prosecution	**VELM Article 1 §1:** These norms apply to reports regarding clerics or members of Institutes of Consecrated Life or Societies of Apostolic Life and Moderators of international associations of the faithful recognised or erected by the Apostolic See concerning: b) conduct carried out by the subjects referred to in art. 6, consisting of actions or omissions intended to interfere with or avoid civil investigations or canonical investigations, whether administrative or penal, against one of the subjects indicated in §1 regarding the delicts referred to in letter a) of this paragraph.
ROI: Children First Act 2015 **NI: Mandatory Reporting (Specific Roles):** The Protection of Children and Vulnerable Adults (NI) Order 2003 requires childcare organizations to report to the Department of Health, Social Services and Public Safety (DHSSPS) if an employee in a regulated position has harmed a child or placed them at risk	**VELM Art. 3 – Reporting** §1. Except for when a cleric learns of information during the exercise of ministry in the internal forum, whenever a cleric or a member of an Institute of Consecrated Life or of a Society of Apostolic Life learns, or has well-founded motives to believe, that one of the acts referred to in art. 1 has been committed, that person is obliged to report it promptly to the local Ordinary where the events are said to have occurred or to another Ordinary among those referred to in canons 134 CIC and 984 CCEO, except for what is established by §3 of the present article. §2. Any person, in particular the lay faithful who serve in offices or exercise ministries in the Church, can submit a report concerning one of the acts referred to in art. 1, using the methods referred to in the preceding article, or by any other appropriate means. §3. When the report concerns one of the persons indicated in art. 6, it is to be addressed to the Authority identified on the basis of articles 8 and 9. The report can always be sent to the competent Dicastery directly or through the Pontifical Representative. If the first option is chosen, the Dicastery will inform the Pontifical Representative about the matter. §4. The report must include as many particulars as possible, such as indications of time and place of the facts, of the persons involved or informed, as well as any other circumstance that may be useful in order

	to ensure an accurate assessment of the facts. §5. Information can also be acquired *ex officio*.
ROI: Data Protection Act 2018 Article 6 (c) **NI:** Article 6(1)(c) of the UK GDPR stipulates that processing is lawful if it is necessary for compliance with a legal obligation (excluding contractual obligations).	**Can. 1284 §1** All administrators are to perform their duties with the diligence of a good householder. **§ 2** Therefore they must: **1º** be vigilant that no goods placed in their care in any way perish or suffer damage; to this end they are, to extent necessary, to arrange insurance contracts; **2º** ensure that the ownership of ecclesiastical goods is safeguarded in ways which are valid in civil law; **3º** observe the provisions of canon and civil law, and the stipulations of the founder or donor or lawful authority; they are to take special care that damage will not be suffered by the church through the non-observance of the civil law; **9º** keep in order and preserve in convenient and suitable archive the documents and records establishing the rights of the church or institute to its goods; where conveniently possible, authentic copies must be placed in the curial archives.

8. Data Breach

A data breach is a security incident where confidential, sensitive, or protected information is accessed, disclosed, altered, lost, or destroyed without the permission of the owner. It is essentially information falling into the wrong hands.

Data breaches can be caused by malicious external cyberattacks (like phishing or malware), malicious insiders, or even accidental human error (such as an employee sending an email to the wrong person or losing a work laptop).

The primary risk for individuals affected is identity theft, financial fraud, and loss of privacy, while organisations face financial losses, legal penalties, and severe damage to their reputation

Data breaches impacting the Catholic Church involve unauthorised access to sensitive parishioner or congregation data. Breaches often occur due to human error, such as sending data to the wrong recipient, losing devices, or unauthorised access.

Preventing data breaches requires implementing strong password policies, limiting access to sensitive files, using BCC for group emails, securing physical documents, and ensuring compliant data disposal. Adhering to GDPR, training staff, updating software, and securing CCTV systems are also critical steps.

Key prevention measures

- Passwords & Authentication: Use strong, unique passwords for all devices (laptops, phones, computers) and implement multi-factor authentication (MFA) where possible.
- Limit Access: Restrict access to personal data (both digital and paper files) to only those who need it for their roles.
- Physical Security: Lock all filing cabinets containing personal data and ensure office areas are secured when unoccupied.
- Safe Remote Working: Ensure staff working from home keep files private from family members, use dedicated work devices, and follow strict security protocols.

Digital Data Management:

- Email Safety: Always use BCC (Blind Carbon Copy) when sending group emails to avoid disclosing recipient email addresses to others.
- Software Updates: Keep antivirus software, operating systems, and applications updated to close security gaps.
- Data Minimisation: Do not retain personal information longer than necessary.

Breach Reporting: Document all breaches locally and report serious ones in the Republic of Ireland are reported to the Data Protection Commission (DPC) within 72 hours if risk exists, while breaches in Northern Ireland are reported to the Information Commissioner's Office (ICO).

Data access by data subject

If the data subject seeks access to their record which it is important to remember they are entitled to do at any point, the following should take place:

- The contents of the file should be reviewed and assessed so that data belonging to third parties is redacted.
- At an agreed time and place, the file should be made available for reading by the data subject, under the supervision of the bishop, superior or the designated liaison person;
- The data subject can make notes and can ask for notes to be included in the file. If agreed, an amendment can be made to the file note. The file manager should state in writing the reason for the amendment, and sign and date their written note. Any such amendments should also be signed and dated by the data subject.

If there is a disagreement concerning the amendment of any file, and a data controller believes the data is accurate and refuses to change it, they must inform the individual why. Good practice would involve the data controller placing a dated note on the file stating that the individual disputes the accuracy of the data. Furthermore, transparency would involve providing a copy of the data subject ensuring the individual knows exactly what note has been appended to their file.

9. Data Destruction

Data destruction is the secure, irreversible removal of data from storage media to prevent unauthorised access, theft, or data breaches, often required for legal compliance. Common methods include physical shredding, degaussing, and software-based erasure (overwriting). It is crucial for protecting sensitive information during IT asset disposal.

Security Compliance: Regulations like the Data Protection Act require companies to securely dispose of data to prevent breaches.

Preventing Misuse: Deleting files (e.g., emptying the recycling bin) does not erase them; destruction is required to prevent recovery of sensitive, financial, or personal information.

Environmental Responsibility: Secure destruction services often include environmentally friendly disposal or recycling of IT equipment

Key Exceptions

While most administrative data must be deleted, certain religious records have permanent or long-term retention requirements:

- **Sacramental Registers:** Records such as baptismal registers are typically permanently retained for the administration of sacraments; individuals do not have a "right to erasure" for these specific entries.
- **Safeguarding Records:** Case management and child safeguarding files are often retained for exceptionally long periods, such as **100 years**, and should not be destroyed without expert review.

Maintaining a log (or certificate of destruction) is considered best practice under data protection regulations like the GDPR, to prove that records have been securely and appropriately disposed of once their retention period has ended.

While the GDPR does not explicitly mandate a log in all circumstances, a destruction log could be evidence of demonstrating accountability in data protection.

A destruction log might contain.

Reference: File number or specific description of the records.

Former Location: Where the file was stored before destruction.

Date: The exact date the data was destroyed.

Title/Type: A clear title for the record being deleted.

Authority: The name of the person who authorised the destruction.

10. Conclusion

A robust approach to data protection, retention, and destruction is no longer optional, it is a fundamental requirement for any organisation operating in an increasingly data-driven world.

Data protection within the Catholic Church is not merely a legal obligation but an expression of its moral and pastoral mission. By upholding principles such as transparency, accountability, purpose limitation, and respect for individual dignity, the Church demonstrates that safeguarding personal information is inseparable from safeguarding the children and young people it serves.

These principles help ensure that the faithful can engage confidently in the life of the Church, knowing their privacy is treated with integrity and care. As digital technologies continue to evolve, the Church's commitment to responsible data stewardship must remain dynamic, rooted in its ethical tradition while responsive to contemporary challenges. In doing so, the Church not only complies with civil regulations but also embodies its deeper calling to protect the vulnerable, promote trust, and honour the inherent worth of every person.

FURTHER SUPPORT
For more advice and guidance on data retention and destruction, please contact:

Republic of Ireland	Data Protection Commissioner: https://www.dataprotection.ie Tusla information and advice officers: http://www.tusla.ie/children-first/roles-andresponsibilities/organisations/children-first-training
Northern Ireland	Information commissioner: https://ico.org.uk Department of Health, Social Services and Public Safety (DHSSPS): http://www.dhsspsni.gov.uk/index/gmgr.htm

REFERENCES

1 Data Protection Commission. (n.d.). *Data protection impact assessments*. Retrieved May 22, 2026, from http://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments.

2 European Parliament and Council of the European Union. (2016). General Data Protection Regulation (GDPR), Article 4(1). General Data Protection Regulation (EU) 2016/679.

3 HIQA. (2017). Privacy Impact Assessment toolkit for health and social care. Health Information and Quality Authority (HIQA)

4. Data Protection Commission. (n.d.). Guidance on legal bases for processing personal data. http://www.dataprotection.ie/en/dpc-guidance/guidance-legal-bases-processing-personal-data

5. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88.

6. Data Protection Act 2018, No. 7/2018, Dublin: Stationery Office, http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/htm

7. Data Protection Act 2018, c. 12, Available at: https://www.legislation.gov.uk/ukpga/2018/12

8. Data Protection Act 2018, No. 7/2018, Dublin: Stationery Office, http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/htm

9. European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, and the Statutory Instrument (S.I.) Number: S.I. No. 336/2011. These regulations were published on July 5, 2011 and enact Directive 2002/58/EC as amended by Directive 2009/136/EC

10. Data Protection Act 2018, c. 12, Available at: https://www.legislation.gov.uk/ukpga/2018/12

11. Privacy and Electronic Communications (EC Directive) Regulations 2003, S.I. 2003/2426. https://www.legislation.gov.uk/uksi/2003/2426/contents Legislation.gov.uk

12. Freedom of Information Act 2000, c. 36. Legislation.gov.uk

13. Charter of Fundamental Rights of the European Union, 2012/C 326/02, 14 December 2007, Art. 8, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT EUR-Lex

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

*15. **Data Protection Acts 1998-2003** Irish legislation can be found on the official Irish Statute Book website.*

16. Code of Canon Law, c. 487, §2, in Code of Canon Law: Latin-English Edition (Washington, DC: Canon Law Society of America, 1999)

Appendix 1: Sample Retention Schedule of Safeguarding Documents

CHILDREN'S/YOUNG PEOPLE'S ACTIVITIES: PARISH/COMMUNITY OFFICE		
Document	**Lawful basis for Processing**	**Suggested retention Period**
Parental consent forms or Joint Child/Young Person &/Parent consent forms for participation in activities *These forms record parent/guardian's consent for child to participate in an activity; the child or young person's consent for their participation; parent/guardian contact details; children's medical and dietary requirements*	Safeguarding/duty of care GDPR Basis: Article 6(1)(c)- Legal obligation Article 6(1)(f)- legitimate interests (protecting children)	6 years Because issues might arise after the activity has ended
Attendance sheets *These record the attendance of children and adults participating in parish/community activities involving children*	Children First Act 2015 Safety, Health & Welfare at Work Act 2005 Statute of Limitations 1957 Allow the organisation to respond to any safeguarding, safety, or legal issues that may arise after the event GDPR: Article 6(1)(c)- Legal obligation & Article 6(1)(f)- Legitimate interests (protecting children)	6 years Because issues might arise after the activity has ended
Sacristy sign-in form/book *A record of attendance in the church sacristy*	GDPR: Article 6(1)(f)- legitimate interests (protecting children) Research demonstrates that disclosures of abuse may occur many years or decades after the event occurs. Sacristy records may be required to inform retrospective safeguarding investigations and identify potential witnesses	30 years after the date of the final entry, then review for destruction or continued retention
Risk Assessment *Written risk assessment identifying potential risks of harm to children and the procedures in place to manage those risks*	Children First Act 2015	Review annually Retain indefinitely
Accident/Incident Form *A record of minor incidents or accidents involving children including the response of group leaders*	GDPR: Article 5(2) - Accountability, Article 6(1)(c)- Health and Safety duties & Article 6(1)(f)- Legitimate interests (protecting children)	Minor incidents/ accidents- 6 years Serious incidents/ accidents- until the child is 18 plus 2 years

General Complaints Form *(not abuse allegations)* *A record of concerns or dissatisfaction raised by children or by parents/ guardians in relation to their children which necessitates a formal response*	Article 6(1)(f)- Legitimate interests	6 years from complaint closure date (or longer if there are legal proceedings)
External Use of Church Property Forms *A record of an external agency's Child Safeguarding Statement and insurance policy*	GDPR: Article 5(2) - Accountability, Article 6(1)(c)- Health and Safety duties & Article 6(1)(f)- Legitimate interests (protecting children)	Renew annually 6 years after final use because issues might arise after the activity has ended

RECRUITMENT: DIOCESEAN/PROVINICAL/SECTOR/PARISH OFFICE		
Document	**Lawful basis for Processing**	**Suggested retention Period**
Application Forms- Staff & Volunteers	Paid Staff- GDPR: Article6(1)(b)-contract Volunteers- GDPR: Article 6(1)(f)- Legitimate interests	Unsuccessful applications- 1 year after recruitment process to allow responses to any disputes
Garda Vetting	National Vetting Bureau (Children and Vulnerable Persons) Acts 2012-2016.	Delete Garda vetting disclosures a year after the end of the employment, except in exceptional circumstances. The reference number and date of a disclosure can be kept for future reference
AccessNI Forms	The Police Act 1997 (Criminal Records) (Disclosure) allows for an enhanced criminal record check for those engaged in regulated activities with children and vulnerable adults. The Safeguarding Vulnerable Groups (Northern Ireland) Order 2007 sets out the activities and work that are 'regulated activities'	The authorised signatory retains a record of the reference number and the date when the Vetting Disclosure Certificate was presented. No longer than 6 months
Police Clearance Certificates (Copy)	GDPR: Article 6(1)(c) - Legal Obligation Article 6(1)(e) - Public Task Article 10 - Criminal Convictions	Delete Police Clearance Certificates 1 year after the end of the employment, except in exceptional circumstances.

Declaration Forms *Witten statement confirming whether or not an applicant has any criminal convictions or investigations relevant to working with children*	GDPR: Article 6(1)(c) - Legal Obligation Article 6(1)(e) - Public Task Article 10 - Criminal Convictions	1 year after the end of the employment, except in exceptional circumstances.
Induction Agreement *Written agreement that the individual has completed safeguarding induction and understands their role, responsibilities and expected standards of behaviour*	GDPR: Article 6(1)(b) - Performance of a Contract Article 6(1)(c) - Legal Obligation Article 6(1)(f) - Legitimate Interests	1 year after the end of the employment, except in exceptional circumstances
Code of Behaviour *Written agreement to adhere to the expected standards of conduct and boundaries for personnel when working with children*	GDPR: Article 6(1)(f)- Legitimate interests (protecting children)	1 year after the end of the employment, except in exceptional circumstances

CASE MANAGEMENT MATERIAL: DIOCESEAN/PROVINCIAL/SECTOR OFFICE		
Document	**Lawful basis for Processing**	**Suggested Retention Period**
Case file in the name of the alleged perpetrators	GDPR Article 6.1 (d) – *processing is necessary in order to protect the vital interests ….of another natural person*	Indefinitely
Case information reported to the diocese/congregation that does not involve case management by a Church body, but where a statutory notification is made	Article 6(1)(f) - Legitimate Interests (protecting children)	Indefinitely

Published 2026

Copyright © The National Board for Safeguarding Children in the Catholic Church in Ireland, 2026

The material in this publication is protected by copyright law. Except as may be permitted by law, no part of the material may be reproduced (including by storage in a retrieval system) or transmitted in any form or by any means, adapted, rented or lent without the written permission of the copyright owners. Applications for permissions should be addressed to the publisher.