GENERAL DATA PROTECTION REGULATIONS AND SAFEGUARDING (RI)

Data Protection Legislation sets out rules relating to the protection of personal data. Data Protection Legislation includes the Irish Data Protection Act 2018 and any regulations or enactments thereunder; Regulation (EU) 2016/679, the General Data Protection Regulation ("GDPR"). These rules aim to protect the fundamental rights and freedoms of people in relation to their personal data. We all have a responsibility to protect the personal data that we collect and use. Personal data, in this context, means any information relating to an identified or identifiable natural person.

Data Protection Legislation outlines principles that you need to follow when processing personal data. Personal data must be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specific, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Only stored for as long as is necessary.
- Processed in a manner that ensures the personal data is kept safe and secure.

You are responsible for and need to demonstrate compliance with the principles outlined above, at all times. If these regulations are not adhered to, and you are not able to demonstrate the activities you have undertaken to be compliant, financial penalties of up to €20million or 4% of annual turnover are possible, whichever is highest. Therefore, we all need to take the protection and management of personal data seriously.

In broad terms, there are six ways that you can lawfully use personal data[1]. At least one of these six factors must be present when using people's personal data and document how and why this particular method was chosen[2]. For example, if you decide to use consent[3], you need to get permission from the individuals involved to use their personal data and tell them what you are using it for. By doing this you can increase the likelihood of it being found that you are processing personal data lawfully. Similarly, if you rely on legitimate interest you need to document that you have undertaken the legitimate interest test and show that it is necessary to process information in this way. By doing this you can increase the likelihood of it being found that you are processing personal data legally[4]. However, the particular circumstances in which personal data is proposed to be processed may affect the legality of that processing and where you have any doubt, you should seek specific legal advice prior to beginning that processing.

[1] See Article 6, GDPR.
[2] Consent, legitimate interest, contractual necessity, public interest, compliance with legal obligation, vital interest
[3] Consent must be freely given and can be withdrawn at any time. If an individual withdraws consent, you may no longer process their personal data unless another lawful basis applies.
[4] Legitimate interest may in some instances be the most flexible way to process personal data. However, you cannot always assume it can be used. It is often most appropriate to use where you use personal data in ways people would reasonably expect, which has a minimal impact on their privacy and/or where there is a compelling justification for the processing. However, this involves considering whether *"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child"*, meaning that it is a nuanced test.

Within data protection legislation, children and vulnerable adults merit specific protection, as they may be less aware of the risks, consequences and safeguards concerned, and their rights in relation to the processing of their personal data. Explicit consent is always required to process information about children and vulnerable adults and any data protection information notices should be written with this audience in mind. Note: under Data Protection Act 2018, a child is anyone under the age of 18 years.

Data Protection Legislation also gives individuals enhanced rights to know how their personal information is being used, including the right to be informed about what their personal data is being used for, have access to a copy of their personal data, request to have personal data amended and erased, restrict and object to their personal data being used, and can request for their personal data to be in an accessible and portable format (e.g. online) so it can be transferred to another organisation if requested.

Safeguarding Trust, the Church of Ireland's child safeguarding policy, and Adult Safeguarding, the Church of Ireland's vulnerable adults policy puts procedures in place to create a safe environment for the protection of children and vulnerable adults. Information in relation to children (and their parents/guardians) must be kept safely and securely, only shared with people who 'absolutely need to know', is accurate and up to date and is not stored for longer than is necessary. You must not keep personal data for longer than you need it and you need to think about, and be able to justify, how long you are holding onto personal data. This depends on the purpose for holding the personal data in the first place.

Safeguarding Trust and *Adult Safeguarding* requires you to secure and protect sensitive personal data. You must have appropriate safeguards in place including:

PHYSICAL SECURITY

- Access to any areas used to store personal information should be restricted.
- All related documents, information, correspondence should be stored in locked filing cabinets.
- A register of issued keys should be created and maintained to ensure no unauthorised access to secure storage areas or buildings.
- You may decide to undertake a risk assessment[5] regarding access to your facilities. Some solutions to physical access concerns include a secure door access system or CCTV.

IT SECURITY

- All staff and volunteers should use a unique user name and password to access safeguarding records.
- User accounts and passwords should not be shared and regularly changed.
- All computer systems should be locked when unattended and set to automatic lock after a set period of time.

[5] Data Privacy Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks

- *Safeguarding Trust* data should be backed up regularly.
- Any portable computer equipment, e.g. laptops, tablets, holding *Safeguarding Trust* material, should have full disk encryption enabled where possible.
- Panel members should work with the Select Vestry to ensure that safeguarding data on electronic platforms is adequately protected, including confirming that:
  - All computer systems should be running on currently supported operating systems and applications. E.g. Windows Vista and Microsoft Office 2007 are no longer supported by Microsoft and security updates are no longer published.
  - All computer systems used for *Safeguarding Trust* should be running anti-malware (anti-virus) software.
  - All computer systems and their software applications where *Safeguarding Trust* information is stored should be patched (updated) regularly - enabling automatic updates is the recommended solution.
  - Software installed on computer systems should be limited to what is required to deliver the required operations. More software can mean greater risk.

If these safeguards are not followed, a personal data breach may occur. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. Immediate remedial action is required if this happens[6]. Where a serious personal data breach occurs, you must, without undue delay and where feasible within 72 hours of becoming aware of the breach, notify the Data Protection Commission of the breach[7] unless, taking into account the nature of the personal data and the scope, context and purposes of the processing, the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. Any decision not to report a data breach to the Data Protection Commission must be recorded with the provision of reasons for such decision.

There are also specific rules in relation to mobile phones and photography. Photographs should be treated the same as you would any other sensitive personal data. Explicit consent is always required before photographs of children/minors can be taken, used and stored. Parents/guardians also need full transparency on how these images will be used and need to be given the option to give partial consent; full consent and/or withdraw their consent.

HOW LONG DO YOU NEED TO HOLD ONTO INFORMATION?

You need to follow retention guidelines for the *Safeguarding Trust* and *Adult Safeguarding* records that you hold. Below you will find some guidelines that you can follow. If, at a local level, you determine the need to hold onto records longer then outlined, please document the rationale behind this. When you archive information, it is important to keep a list of what documents have been archived, the date of archive and the location of storage. This will ensure you can retrieve

[6] You need to develop a data breach procedure; keep a log of all data breaches; if significant risk you may need to contact the Data Protection Commission (ROI) / Information Commissioner's Office (NI)
[7] Section, Data Protection Act 2018

the information if/when you need to. You can also keep personal data longer if you regard the information as important for public interest, or historical research. If you decide to anonymise the personal data when you no longer need it, you can also hold onto it indefinitely.

RETENTION GUIDELINES

Type of Record	Responsibility	Details of records	Retention period
Child Protection Records	The Select Vestry (through the Panel) is responsible for managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Any disclosures, concerns or allegations of child abuse • Any records relating to disclosures, concerns or allegations including reports from bishops/clergy/staff/volunteers, reports and correspondence to/from Tusla, reports to An Garda Síochána • Any records of advice given to bishops/ clergy/staff/volunteers and notifications to parents in relation to a concern, disclosure or allegation • Any complaints about the safety and welfare of children while at children's ministry activities • Any protective measures or action taken in relation to an allegation against a staff/ volunteer • Any actions taken in response to a complaint against staff/volunteer	Keep indefinitely and archive
Adult Protection Records	The Diocesan Panel are responsible for dealing with adult protection records but Select Vestries must ensure they have all relevant information available to the Diocesan Panel	• Any disclosures, concerns or allegations of abuse • Any records relating to disclosures, concerns or allegations including reports from clergy/staff/volunteers, reports and correspondence to/from HSE, reports to the Gardaí • Any records of advice given to clergy/ staff/volunteers and • Any complaints about the safety and welfare of adults while at ministry activities • Any protective measures or action taken in relation to an allegation against a staff/ volunteer • Any actions taken in response to a complaint against staff/volunteer	Keep indefinitely and archive
Information on children and young people	The Select Vestry (through the Panel) is responsible for managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Membership / Registration forms	Archive until 7 years after the child turns 18 years then: Keep a reduced register of members (see sample below) including name, address and date of birth and dates of membership to be archived indefinitely; and delete all other material
		• Accident reporting sheet of books of children	The date when a child become an adult plus 20 years then destroy
		• Attendance records	Archive indefinitely
		• Other parental consent forms	Archive until 7 years after the child turns 18 years, then destroy

Type of Record	Responsibility	Details of records	Retention period
Information on adults who may potentially be at risk	The Select Vestry is responsible for ensuring compliance with the managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Membership/ Registration forms	Keep a reduced register of members (see sample below) including name, address and date of birth and dates of membership to be archived indefinitely; and delete all other material
		• Accident reporting sheets or books	20 years then destroy
		• Attendance records	Archive indefinitely
Personnel Records Staff	The Select Vestry (through the Panel) is responsible for managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Terms and conditions of employment (details, references, pay, etc)	Throughout employment and then for 6 years then destroy
		• Policies	Indefinitely, archive
		• HR Records (annual leave/ sick leave)	Throughout employment plus 6 years then destroy
		• Disciplinary records	Duration of employment plus 6 years after resignation / retirement then destroy. Where criminal activity, hold indefinitely.
		• Carers Leave / Parental Leave / Maternity Leave records	Throughout employment. The records should be retained for 8 years following the last date leave was taken, then destroyed.
		• Job description and files	Archive
		• Job competition files (all called for interview)	2 years after competition is closed, then destroy apart from those employed.
		• Selection Criteria	Archive
		• Candidates short-listed but are not successful and/ or do not accept role.	2 years and then destroy.
		• Interview board marking sheets and interview board notes	2 years and then destroy.
		• Panrel recommended by interview board, promotion files, reports.	Archive
		• Garda Vetting Related Information - Nil disclosure returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then record date vetted, outcome of disclosure and archive indefinitely. Destroy all other documents.
		• Garda Vetting Related Information - Disclosure with Criminal Record returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then destroy Vetting Invitation form and ID documents. Archive Vetting Disclosure indefinitely.
		• Annual appraisal, declaration of acceptance and training records	Archive indefinitely

	Responsibility	Details of records	Retention period
Personnel Records - Volunteers	The Select Vestry (through the Panel) is responsible for managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Volunteer Agreement	Throughout volunteering and then for 6 years after. Keep name, date of appointment and departure on volunteer register (see sample below) and archive indefinitely. Destroy agreements.
		• Application form	Throughout volunteering and then for 6 years: Keep name, address and date of birth on volunteer register. Archive indefinitely. Delete all other material
		• Policies	Archive indefinitely
		• Disciplinary records	Duration of employment plus 6 years after resignation / retirement then destroy. Where criminal activity, hold indefinitely
		• Role descriptions and files	Archive indefinitely
		• References	Throughout volunteering and then for 6 years: Keep a detail of whom references received from, date and whether they were favourable on volunteer register. Archive indefinitely. Destroy references.
		• Interview records and panel recommendation	Archive indefinitely
		• Annual Review forms	Throughout volunteering and then for 1 year then destroy.
		• Declaration of acceptance and training records	Throughout volunteering and then for 6 years. Keep details of date of declaration and last training attended on volunteer register to be archived indefinitely. Destroy all forms.
		• Garda Vetting Related Information Nil disclosure returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then record date vetted, outcome of disclosure and archive indefinitely. Destroy all other documents.
		• Garda Vetting related information – Disclosure with Criminal Record returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then destroy Vetting Invitation form and ID documents. Archive Vetting Disclosure indefinitely.

Personnel Records - Junior Helpers (under 18s)	The Select Vestry (through the Panel) is responsible for managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Garda Vetting Related Information - Nil disclosure returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then record date vetted, outcome of disclosure and archive indefinitely. Destroy all other documents.
		• Garda Vetting related information – Disclosure with Criminal Record returned	Retain original signed Vetting Invitation form, copies of ID and Vetting Disclosure for lifetime of the vetting application, i.e. until the person is re-vetted, resigns or ends his/her involvement with your organisation. Then destroy Vetting Invitation form and ID documents. Archive Vetting Disclosure indefinitely.
		• Information on young people (volunteers under 18 years)	Retain and then destroy: hold for 7 years after they turn 18 years and move onto an adult volunteer agreement. Keep indefinitely: name, date of birth, a record of the dates and activities participated in; including record of attendance.

TOP TIPS TO BECOMING COMPLIANT

(a) Ensure your panel knows their roles and responsibilities under Data Protection law.

(b) Review all the safeguarding information you hold and ensure you are working within retention guidelines.
- Archiving can be within the panel's *Safeguarding Trust* filing cabinet or to electronic format as per guidance in SGT policy.

(c) Develop clear privacy notices both generally and for children and vulnerable adults so that they are able to understand what will happen to their personal data, and what rights they have.

(d) Develop and implement your security plans - both physical and IT.

(e) Develop a plan on how to manage a data breach *https://www.ireland.anglican.org/cmsfiles/pdf/Resources/ParishResources/SelectVestry/GDPR/DataBreachGuide.pdf.*

(f) Develop a plan on how to manage a subject access request (when someone asks for the personal data you hold on them) *https://www.ireland.anglican.org/cmsfiles/pdf/Resources/ParishResources/SelectVestry/GDPR/SubjectAccessRequest.pdf*

(g) Undertake Data Privacy Impact Assessment as/if required (risk assessment).

(h) Develop a cyclical review process to regularly review your data protection practices and ensure all personal information is adhering to data protection principles.

Parishes should have steps c - h in place already as part of their GDPR responsibilities.

If you have any questions or queries, please visit our website: *www.ireland.anglican.org/parishresources*. Alternatively contact our data protection officer by emailing dataprotection@rcbcoi.org.

Alternatively, the supervisory authority for the Church of Ireland is the Office of the Data Protection Commissioner. Their contact details are: 6 Pembroke Row, Dublin 2, D02 X963, Ireland; https://dataprotection.ie/en/contact/how-contact-us.

SAMPLE VOLUNTEER REGISTER

Parish of .....

Name of Volunteer		
Address		
Date of Birth		
Volunteer Role		
Name of Referee (1)		
Date of reference		
Was reference favourable	YES ❑	NO ❑
Name of Referee (2)		
Date of reference		
Was reference favourable	YES ❑	NO ❑
Date of last vetting disclosure		
Any negative disclosure	YES ❑	NO ❑
Date of Appointment		
Date of declaration of acceptance		
Date of last SGT training attended		
Date of Resignation		

To be completed for each volunteer and kept indefinitely (even after original forms are destroyed in line with GDPR & SGT Guidelines).

SAMPLE REGISTER FOR MEMBERS COMPILED FROM MEMBERSHIP / REGISTRATION FORMS

Name of Group .....

Year of Membership .....

Name of Member	Address of Member	Date of Birth of Member

To be completed for each group before Membership/Registration forms are destroyed in line with GDPR & SGT Guidelines.