GENERAL DATA PROTECTION REGULATIONS AND SAFEGUARDING (NI)

Data Protection Legislation, most recently the General Data Protection Regulation (GDPR) (2018) and together with the Data Protection Act 2018 sets out rules relating to the protection of personal data. We have a responsibility to protect the personal data that we collect and use. The regulation outlines data protection 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.

Within data protection legislation, children and adults at risk 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 adults at risk and any data protection information notices should be written with this audience in mind. Note: under GDPR, a child is anyone under the age of 13 years. GDPR 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 protection policy, puts procedures in place to create a safe environment for the protection of children and young people. 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. This depends on the purpose for holding the personal data in the first place. *Safeguarding Trust* requires you to hold onto sensitive personal data. You must have appropriate safeguards in place including:

PHYSICAL SECURITY

- Any areas used to store personal information should be kept locked when not occupied.
- 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[1] regarding access to your facilities. Some solutions to physical access concerns include a secure door access system or CCTV.

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

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.
- Passwords should be changed on a regular basis.
- All computer systems should be locked when unattended and set to automatic lock after a set period of time.
- *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 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, you may find yourself dealing with a personal data breach. 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[2].

HOW LONG DO YOU NEED TO HOLD ONTO INFORMATION?

You need to follow retention guidelines for the *Safeguarding Trust* 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 offsite storage (e.g. Child Protection Records, 2006-2008, RB Library). This will ensure you can retrieve the information if/when you need to. You can also keep personal data longer

[2] You need to develop a data breach procedure; keep a log of all data breaches; if significant risk you may need to contact the Information Commissioner's Office (NI)

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 Parish Panel) is responsible for ensuring compliance with the 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 workers/volunteers, reports and correspondence to/from Gateway (Social Services), reports to the PSNI • Any records of advice given to 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 workers/volunteers, reports and correspondence to/from Gateway (Social Services), reports to the PSNI • Any records of advice given to 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 Parish Panel) is responsible for ensuring compliance with the 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 sheet or books	20 years then destroy
		• Attendance records	Archive indefinitely
Personnel Records Staff	The Select Vestry (through the Parish Panel) is responsible for ensuring compliance with the 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 1 year then destroy
		• Policies	Indefinitely, archive
		• HR Records (annual leave / sick leave)	Throughout employment plus 6 years and 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 eight years following the last date leave was taken. Then destroyed.
		• Job descriptions and files	Archive
		• Job competition files (all called for interview)	2 years after competition is closed then destroy except for 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
		• Panel recommended by interview board, promotion files, reports	Archive
		• Access NI checks	Keep record of name, date and fact that they were vetted with no negative disclosure. Delete everything else after one year.
		• Annual Appraisal, declaration of acceptance and training records	Archive indefinitely

Type of Record	Responsibility	Details of records	Retention period
Personnel Records - Volunteers	The Select Vestry (through the Parish Panel) is responsible for ensuring compliance with the managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Volunteer Agreement	Throughout volunteering and then for 1 year 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 1 year: 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 1 year: Keep a detail of who 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 1 year. Keep details of date of declaration and last training attended on volunteer register to be archived indefinitely. Destroy all forms.
Personnel Records - Junior Helpers under 18s	The Select Vestry (through the Parish Panel) is responsible for ensuring compliance with the managing; protecting; limiting access; updating and reporting; adhering to all data principles	• Access NI Checks	Keep record of name, date of vetting and fact that they were vetted with no negative disclosure. Delete everything else after one year.
		• 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 know their roles and responsibilities under Data Protection.

(b) Review all the safeguarding information you hold and ensure you are working within retention guidelines
- The RCB Library may archive records on your behalf. 01-4923979 / library@ireland.anglican.org

(c) Develop clear privacy notices 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.

(f) Develop a plan on how to manage a subject access request (when someone asks for the personal data you hold on them).

(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.

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.