Data Protection Policy

The diocese of Kilmore is required under the Data Protection Acts 1988 & 2003 to ensure the security and confidentiality of all personal data it collects and processes on behalf of its volunteers and employees.

Personal data must be obtained and processed fairly, kept only for one or more specified explicit and lawful purpose, used and disclosed only in ways compatible with the purpose for which it was obtained and, kept safe, secure, accurate, complete and up to date, adequate, relevant and not excessive, retained for no longer than is necessary for the purpose or purposes for which it was collected and may be given to an individual upon receipt of request.

Retention and Security of Records

- File records which contain personal information should be stored in a secured locked file in the Parish Priest's house or Parish Office.
- All personal files must be locked away securely from unauthorised access.
- Access to locked cabinets/filing cabinets must be on a need to know basis only.
- The Parish Priest or his nominee are the only persons who are approved to access personal files.
- All computer/laptops used for the purpose of record keeping must be password protected and encrypted.
- Persons who store information on computers/laptops for the purpose of parish records must use individual passwords and access must only be by the Parish Priest or a nominee.
- Keys to filing cabinets/locked cabinets should be strictly controlled with access provided only to Parish Priest or one named nominee.

Retention and Destruction of Data

- All case management safeguarding files should be retained for a period of 100 years.
- All other files pertaining to safeguarding should be stored for a period of 30 years.
- When volunteers/employees retire from positions/posts, files should be moved to Archive Storage however the same security arrangements as outlined above must apply to these records.
- Where there is no legal requirement to retain records beyond closure, destruction should be undertaken as follows:-
  - An inventory should be completed indicating name of file, location of file, destruction date, method of destruction, signed approval for destruction to be signed off by the Data Controller or nominated persons.
  - Destruction of waste paper/records containing personal information must be by way of incineration or cross shredding.

Access to Information

- Persons wishing to access records should be provided with a copy of their own personal information only.
- Such applications must be in writing.

The right of access does not apply in certain circumstances, where it is likely to prejudice an ongoing investigation.

April 2012