25. Data Security Policy

The Church's information is one of its most critical assets and needs to be both protected and used wisely to support the Church's mission.

Much of our information is held in electronic form requiring action to ensure that data held is both secure and its integrity is maintained. Employees, volunteers contractors and agents play a vital role in making this possible.

This policy should be read in conjunction with the *Use of the Information Technology, Email and the Internet* policy and Diocesan Privacy policy.

25.1. Purpose

The purpose of this policy is to set out the Diocesan Data Security Policy.

This policy is aimed at ensuring all confidential information and personal information is protected from unauthorised and/or accidental disclosure.

25.2. Application

This policy applies to all people in diocesan workplaces including staff (priests, brothers, sisters, seminarians and employees), volunteers, contractors and agents of the Diocese.

25.3. What data is subject to this policy?

This policy refers to all electronic information created or kept by the Catholic Diocese of Ballarat, except for information that is in the public domain (unless it is in the public domain because of a breach of this policy).

Electronic information includes software, intellectual property, manuals, advice, public relations information, contact details. It is stored on local drives, individual PCs, on network directories or applications, finance systems, payroll systems, in online accounts and in "cloud" systems.

25.4. Diocese expectations

All staff, volunteers, contractors and agents are required to adhere to the following expectations in handling the Diocese's electronic information.

- Unless necessary for your duties, do not remove any electronic information from Diocese systems or computers.
- Keep all files (other than your personal information) on a shared drive.
- Use a password that has at mixture of alpha and numerical characters (often this is dictated by the system itself).
- Do not use passwords that can easily be identified, e.g. your name, date of birth.
- Do no leave your password written down where it can be easier accessed.
- Change your password regularly and any time it is compromised or you suspect it may have been compromised.
- Do not give your password to anyone. They should have and use their own log-in and passwords. You are responsible for access obtained and usage under your log-in in and password. The only person that has authorised access to your password is the system administrator.

- Lock your computer if you are going to be away from your workstation for an extended period of time.
- Secure sensitive files with their own password protection.
- When the Catholic Diocese of Ballarat information is stored or transferred for the purpose of legitimately accessing the information off-site, appropriate security protocols must be followed by the carrier of the information, and appropriate security measures must be provided on home computers and/or portable devices such as portable storage devices where diocesan information may be accessed.