Parish Data Protection and Information Technology Checklist

Objective/Intent

The following checklist is intended to provide general information to assist parishes in managing and minimising the risks associated with data protection and information technology. This is not an exhaustive checklist of all possible controls.

Where the parish answers the question with a 'no', further investigation of the risk and possible control measures should be determined and implemented.

Data Protection	Yes	No	N/A	Action Required	Date
Are electronic files backed up or copied regularly?					
Are critical documents stored in lockable fire rated/waterproof filing cabinets?					
Are copies of critical documents stored at an off-site facility?					
Are you aware of the critical IT applications that you need to use on a regular (if not daily basis)? Eg: Parish Census, Rosters and Registers.					
In the event of IT failure or theft, do you have a manual or alternative process to maintain critical business functions?					
Do you know how long it would take to recover IT functions in a crisis? Is the Data readily accessible?					
Do you have the contact details of the individual responsible for restoring your IT systems in the event of failure?					
Is your computer antivirus software up-to-date and licensed?					
Are staff and volunteers aware of email and internet usage policies?					

Disclaimer: This checklist is provided by the Catholic Diocese of Bunbury to its parishes as a courtesy. The checklist is of general nature only and does not consider your personal needs and uses for the information. You should therefore consider this as a guide only and make your own enquiries. The Diocese recommends that you consider seeking professional assistance before making use of and relying on this document.