RISK INFORMATION – CHURCHES
CYBER SERIES – DATA BREACH PLAN

Securing personal information should be an important priority for all Baptist churches and organisations, to protect the privacy of individuals.
From the 22 February 1918, the Commonwealth Government has established a Notifiable Data Breach (NDB) scheme to ensure that affected individuals are advised of serious data breaches.
All organisations subject to the Australian Privacy Act 1988 must advise when a serious data breach occurs.

This risk information document will assist you in developing your Data Breach Plan.

A data breach occurs when personal information held by an entity is lost or subjected to unauthorised access, modification, disclosure or other misuse or interference. Note that a data breach may also constitute a breach of the Privacy Act.

Examples of how a data breach might occur include:

- Lost or stolen computers, iPads or paper records
- Digital storage devices disposed of but contents not erased
- Databases "hacked"
- Employees accessing personal data in an unauthorised manner
- Paper records stolen from bins or recycling
- Mail delivered to the wrong addressee
- Use of deception to access personal information

All organisations subject to the Australian Privacy Act 1988 must advise when a serious data breach occurs. Apart from reporting serious breaches to regulators, affected individuals must also be notified of the data breach.

All churches and Baptist organisations should make sure that potential data breaches are included in their enterprise risk management plans. Existing Privacy policies and procedures will need to be reviewed and may need to be changed..

Churches should develop specific Data Breach Response plans that set out in advance the steps that they will take in the event of a Data Breach occurring. Essential elements to be included in the plan include:

- Definition of what constitutes a breach for your church or organisation
- The strategy to be used to assess, manage and contain a breach – includes staff and external resources
- Reporting lines both internally and externally to relevant regulators

RISK INFORMATION – CHURCHES
CYBER SERIES – DATA BREACH PLAN

- Process to record details of the breach
- Process to identify and remediate control weaknesses
- Post breach review and assessment

The Office of the Australian Information Commissioner has published the following documents to help you in your preparation:

"Notifiable Data Breaches – resources for businesses and agencies"
https://www.oaic.gov.au/engage-with-us/consultations/notifiable-data-breaches/

"Guide to securing personal information – reasonable steps to protect personal information, January 2015" -
https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information

"Guide to developing a data breach response plan, April 2016"
https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-developing-a-data-breach-response-plan