ABOUT NOTIFIABLE DATA BREACHES

A guide for Parishes

Introduction

The purpose of this topic guide is to provide an overview of the new notifiable data breaches (NDB) regime commencing 22 February 2018 and the implications for Parishes.

Under reforms to the Privacy Act, the Diocese now has legal obligations to report and minimise harm to individuals should personal data held by an entity be breached or compromised in some way.

These Federal government changes are in response to the increasing risk of online criminal activity and community concerns about how their personal information is being protected by organisations.

Parish Safe Church programs already include a model Privacy Policy, recognising the need to protect individuals' privacy and the information entrusted to us. This change formalises a data breach reporting procedure and support from the Registry to Parishes in responding to breaches.

What is a data breach?

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. The Parish records may be stored electronically or be paper based. Data breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and have the potential to cause harm to individuals, Parishes and the church.

Some examples of a data breach include:

- where a mobile device such as phone or laptop containing personal information of Parish members is lost or stolen
- where a Parish database containing personal information is hacked
- a Parish makes personal information accessible or visible to others outside the organisation without an individual's permission
- an email containing personal or sensitive information is sent to an external party in error
- unauthorised access to Parish records containing personal information by a church worker or independent contractor

What is personal or sensitive information?

This covers a broad range of information (both fact and opinion) records such as:

- information that identifies that person such as age, gender, address details
- sensitive information such as religious beliefs, criminal record, health information
- banking and credit information
- employee records, tax file numbers etc.

Common examples of personal information

1. **Information about a person's private or family life**
   Persons name, signature, home address, telephone number, date of birth, medical records, bank account details and employment details etc.
2. **Information about a person's working habits and practices**
   A person's employment details, such as work address and contact details, salary, job title and work practice. Details of any loans etc.
3. **Commentary or opinion about a person**
   Records that identify an individual and an opinion that has been given; such as a referees' views of a person's suitability for a role.

What to do if a data breach occurs or is suspected?

If any church worker in a Parish is aware of data breach or suspects a data breach, they should notify the Registrar as soon as possible. A data breach report template is provided on the Diocesan website http://www.bendigoanglican.org.au/ under the Parish Resources section. This template will assist you to gather all relevant information that is known at that time. It may also assist in identifying what immediate remedial action the Parish can take to reduce the risk of potential harm to individuals.

Prompt action is generally the key to reducing the risk of harm. The Registry team will work with the Parish to assess risks and take action, once they have been notified.

Prevention is the best defence

Below are some guidelines that may help Parish Council's assess whether adequate data protection measures are in place to minimise data breach risks:

- Only collect information that is needed and let people know how the data will be used
- Seek permission before sharing personal information
- Reduce the number of places where data is retained
- Delete spam emails and do not open attachments or links from unknown sources
- Grant access to sensitive data on a "needs" basis and with protection measures
- Educate church workers about your Parish's data protection measures
- Keep current records of who has access to data in the Parishes
- Purge records responsibly i.e. don't put personal information is rubbish bins
- Store data securely i.e. locked filing cabinets, or with password protection
- Avoid the risk of hard copy records being left outside the Parish i.e. in cars
- Have electronic backup processes and store back-ups securely
- Encourage discussion of data security concerns, known hoaxes & scams
- Encourage the use of computer security software and regularly install updates
- adopt the revised model Privacy Policy provided by the Diocese and include data protection on you Safe Church Agenda to enable regular reviews and risk mitigation

For further information and implementation support please contact: Deb Allan, Workplace and Project Support Ph 5443 4711 or email hr@bendigoanglican.org.au

External resources available from the Office of Australian Information Commissioner https://www.oaic.gov.au/