PRIVACY POLICY

Document Control Information

This is a document controlled by the Audit, Risk and Compliance Committee (ARCCo).

Review Date

This policy shall be reviewed biennially from the date of approval and all amendments to this policy must be approved by the ARCCo.

Contents

1 INTRODUCTION

The BFS Privacy Policy

- affirms BFS's commitment to protecting and managing personal information held about BFS clients by adherence to the applicable Australian Privacy Principles, procedures and training;
- sets down BFS's obligations under the Privacy Act 1988, the Australian Privacy Principles (APP) and The Privacy Amendment (Notification of Data Breaches) Act 2017 (Commonwealth); and
- aims to provide an understanding of the Australian Privacy Principles including personal information management and security, and how they impact on BFS's operations.

2 LEGAL REQUIREMENTS

The Privacy Act 1988 (Commonwealth) as amended, includes the Australian Privacy Principles as detailed in this Policy, and sets the standards for the way organisations handle personal information. The Privacy Act also gives the office of the Australian Information Commissioner a general power to make Guidelines to help organisations avoid breaching the Act.

The Privacy Amendment (Notifiable Data Breach) Act 2017 (Commonwealth) established the Notifiable Data Breach (NDB) scheme in Australia. The NDB scheme applies to BFS and BFS's personal information security obligations under The Privacy Act 1988 (Commonwealth).

3 STRATEGIC AND ORGANISATIONAL CONTEXT

BFS is a public company limited by guarantee and a Registered Charity. 'BFS' is a registered trademark. BFS has been endorsed by the Australian Charities and Not-for-Profits Commission (and formerly, the Australian Taxation Office) as an Income Tax Exempt Charitable Institution based on Advancement of Religion for the operation of financial services.

BFS is a Religious Charitable Development Fund as defined by the Australian Prudential Regulation Authority (APRA). Such funds are established by religious organisations for seeking investments from the public to make loans that further the religious and charitable goals and objectives of the fund (BFS). This fundraising activity comes within the definition of banking business under the Banking Act 1959, and APRA has exempted BFS from the requirement to be authorised under the Banking Act. Accordingly, BFS is not prudentially supervised by APRA, and contributions to BFS do not obtain the benefit of the depositor protection provisions of the Banking Act 1959. BFS is also a charity for the purposes of Regulatory Guide 87 issued by the Australian Securities & Investments Commission ('ASIC').

4 SUMMARY OF THE AUSTRALIAN PRIVACY PRINCIPLES (APPS)

4.1 APP1 – OPEN & TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

Personal information about an individual must be managed (i.e. collected/used/held etc.) in an open and transparent way. An organisation must have a publicly available policy document regarding its management of personal information held/used/collected.

4.2 APP2 – Anonymity and pseudonymity

Individuals must be given the option of protecting their anonymity wherever possible and lawful by withholding their personal information or using a pseudonym. That is, organisations must ensure personal (identifying) information is only requested from an individual where necessary.

Generally, use and disclosure of information provided will be restricted to the primary disclosed purpose for which it has been collected, unless the individual has consented to its use for a secondary purpose. Sensitive information about an individual is not to be collected without their consent, and unless it is required by law or emergency (such as imminent threat to life/health).

4.3 APP3 – Collection of solicited personal information

An organisation must not collect personal information unless it is reasonably necessary for one or more of the entity's functions or activities. Sensitive information can only be solicited (and provided with consent) if it is reasonably necessary for or directly related to the entity's functions or activities.

4.4 APP4 – Dealing with unsolicited information

Where an organisation receives unsolicited personal information, it must determine whether it could have been collected in line with APP3 above. If the answer is no, it must destroy or de-identify the information.

4.5 APP5 – Notification of collection of personal information

An organisation must notify or make individuals aware that they are collecting personal information when or before they collect it. If not possible, then as soon as reasonably practicable afterwards.

4.6 APP6 – Use and disclosure of personal information

Generally, use and disclosure of information provided will be restricted to the primary disclosed purpose for which it has been collected, unless the individual has consented to its use for a secondary purpose. Sensitive information about an individual is not to be collected without their consent, and unless it is required by law or emergency (such as imminent threat to life/health).

4.7 APP7 – Direct Marketing

Organisations which hold personal information cannot use it for direct marketing purposes unless they have consent to do so, or this would be reasonably expected by the individual, and they have the opportunity to request otherwise (and haven't exercised that right).

4.8 APP8 – Cross Border disclosure of personal information

Personal information about an individual held by an organisation can only be transferred to someone in a foreign country in certain circumstances (e.g. if there is a similarly stringent privacy protection regime binding that foreign country or if the individual consents to the transfer, or if it is in the individual's interest etc).

4.9 APP9 – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

Organisations should not use or disclose identifiers, such as those assigned by Commonwealth agencies (such as a Medicare number or Tax File Number).

4.10 APP10 – QUALITY OF PERSONAL INFORMATION

An organisation must take reasonable steps to ensure that collected, used or disclosed personal information is accurate, complete and up to date.

4.11 APP11 – SECURITY OF INFORMATION

An organisation must ensure the integrity and security of the information collected and stored is protected (from loss, misuse, unauthorised access, disclosure). Information which is no longer needed by an organisation should be destroyed or permanently de-identified.

4.12 APP12 – ACCESS TO PERSONAL INFORMATION

An individual must generally be allowed access to personal information held about them. Please note there is a range of exceptions and limitations on this requirement.

4.13 APP13 – CORRECTION OF PERSONAL INFORMATION

An organisation must correct their records if shown to be inaccurate/incomplete.

5 BFS PRIVACY POLICY

This BFS Privacy Policy sets out in detail the BFS policies on the management of personal information.

This Policy is designed to inform clients of –

- The BFS Privacy Policy;
- What information BFS collects and the purposes for which its collected;
- Use and disclosure of information collected;
- Security of client's personal information;
- Gaining access to information BFS holds about clients;
- What a client can do if they believe the information BFS holds about them is inaccurate;
- Complaints in relation to privacy; and
- How to contact BFS.

This Policy is designed also to inform clients of the obligations BFS has to comply with under the NDB scheme and the procedures BFS will implement and undertake to comply with to meet its obligations under the NDB scheme.

6 PERSONAL INFORMATION

Personal information is information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

BFS will also collect any personal information necessary for the purposes of complying with the Anti-Money Laundering and Counter-Terrorism Financing Act 2006; Anti-Money Laundering and Counter Terrorism Financing Rules and Amendments made under the Act including Anti-Money Laundering and Counter-Terrorism Financing Regulations.

Information generally collected by BFS includes the following (depending on the nature of the service(s) provided):

- client name, address and contact details;
- client e-mail address;
- client tax file number;
- Bank account details;
- Identification and verification information;
- Credit reference information (where applicable); and
- details of specific transactions.

7 OPEN & TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

BFS seeks to ensure that personal information it holds about an individual is managed in an open and transparent manner. BFS has implemented procedures to ensure compliance with the Australian Privacy Principles and any applicable codes, and to deal with any complaints relating to BFS' compliance therewith.

8 COLLECTION OF PERSONAL INFORMATION

This policy details how BFS adheres to the Australian Privacy Principles regarding the collection of solicited personal information. BFS only collects personal information directly from individuals, which is reasonably necessary for the provision of services, and only by lawful and fair means. Information is generally sought through application forms, in which the purpose is articulated. Accordingly, BFS will always ensure clients are apprised of the purpose for collecting information, and their right to gain access to such information. If they do not provide the information requested, BFS may be unable to provide them with services.

Generally, BFS will only use the personal information (e.g. postal address, e-mail address, telephone numbers, facsimile number, date of birth, bank account details, TFN, details related to the provision of credit, verification and identification documentation) collected for the main purposes disclosed at the time of collection such as to provide financial services or credit services.

Where possible BFS will collect the information directly from clients but certain information may be collected about clients from other sources, including a Baptist Union/Association or any Baptist Church or other related, affiliated or associated Baptist body, or for example, a credit reference from a credit reporting agency to obtain information about a client's financial position when they apply for a loan.

9 CREDIT CHECKS

BFS will also collect personal information for Credit Checks which may involve the following:

- obtaining from a credit reporting agency a credit report containing information about a client's personal credit worthiness for the purpose of verifying their identity, assessing their application for a loan and for the purpose of assisting in collecting overdue payments; and

- obtain information about a client's commercial activities or commercial creditworthiness from any business which provides information about the commercial credit worthiness of organisations and persons, an accountant, a Baptist Union/Association or any Baptist Church or other related, affiliated or associated Baptist body, or any other supplier to the client.

Credit reporting agencies will match personal information to information held by the document issuer or official record holder (generally a government agency) for the purposes of verifying the client's identity.

Credit providers like BFS can now provide information about clients to credit reporting bodies, including how much the client has borrowed and whether they fail to meet their loan repayment obligations, in order to enable a more comprehensive credit assessment.

The credit reporting agency BFS use is Equifax Pty Ltd (formerly Veda). You can download a copy of their privacy policies at https://www.equifax.com.au/privacy. A client can request a copy of their credit file from credit reporting bodies and request a copy of the credit-related information BFS hold about them. A client can also request us to correct any inaccurate information or lodge a complaint with BFS relating to such information.

10 UNSOLICITED PERSONAL INFORMATION

Where BFS receives personal information about an individual which is unsolicited and not required for the provision of services, BFS will destroy the information (provided it is lawful and reasonable to do so).

11 NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

When BFS obtains personal information about a client, BFS will ensure that the client has the organisation's contact details and that the client is aware of the collection of information and the purposes for doing so. As per this document, BFS is unable to provide certain services if the requested information is not provided. BFS does not disclose client information to third parties, unless they are related entities or services providers, in which case they are required to conform to BFS' procedures.

12 USE AND DISCLOSURE OF PERSONAL INFORMATION

BFS collects and holds personal information about an individual for the purpose of providing financial or credit services. BFS collects this information with client consent as per the service documentation, for the primary purpose disclosed at the time of collection. We may use and disclose the personal information we collect about you for the following purposes:

- to assist BFS in providing you our products and services;

- completion of documentation and application forms;
- to consider and assess your request for a product or service;
- let you know about other products or services we offer, send you information about special offers or invite you to events;
- to protect our business and other customers from fraudulent or unlawful activity;
- to conduct our business and perform other management and administration tasks;
- to consider any concerns or complaints you may have;
- to manage any legal actions involving BFS;
- to comply with relevant laws, regulations and other legal obligations; and
- to help us improve the products and services offered to our customers, and to enhance our overall business.

However, in some cases BFS will use or disclose personal information for secondary purposes (any purpose other than a primary purpose). Personal information obtained to provide financial or credit services may be applied to secondary purposes if the secondary purpose is related to the primary purpose of collection and the person concerned would reasonably expect the personal information to be used or disclosed for such secondary purpose.

BFS may provide personal information to third parties in order to provide clients with financial services and the provision of credit. The types of organisations to whom we may need to disclose your personal information to include:

- a related entity of BFS;
- an agent, contractor or service provider we engage to carry out our functions and activities, such as our lawyers, accountants, or other advisors;
- organisations involved in a transfer or sale of all or part of our assets or business;
- organisations involved in managing our payments, payment merchants and other financial institutions such as banks;
- regulatory bodies, government agencies, law enforcement bodies and courts;
- your guarantor, referee(s), employer or co-account holder;
- financial product issuers;
- other credit providers and credit reporting bodies;
- a debt collector; and
- anyone else to whom you authorise us to disclose it.

In some cases, BFS may ask clients to consent to any collection, use or disclosure of personal information. Client consent will usually be required in writing but BFS may accept verbal consent in certain circumstances. BFS may also disclose a client's personal information where it is required or authorised by law.

13 DIRECT MARKETING

BFS will only use personal information obtained for the provision of financial or credit services, for the secondary purpose of direct marketing where:

1. BFS collected the personal information from the individual; and
2. The individual would reasonably expect BFS to use or disclose the information for the purpose of direct marketing; and
3. BFS provides a simple means through which an individual can request to not receive marketing communications; and
4. The individual has NOT requested such communications cease.

BFS allows an individual to opt out of the receipt of direct marketing in each direct marketing communication. A client can change their mind about receiving information at any time by contacting BFS on Ph 1300 650 542. Often the law requires BFS to advise clients of certain changes to products/ services or regulations. Clients will continue to receive this information from BFS even if clients choose not to receive direct marketing information from BFS. BFS will not disclose client information to any outside parties for the purpose of allowing them to directly market to clients.

14 CROSS BORDER DISCLOSURE / SENSITIVE INFORMATION / USE OF GOVERNMENT IDENTIFIERS / ANONYMITY & PSUEDONYMITY

BFS may disclose personal information to recipients located outside Australia, including to:

- Service providers or third parties who store data or operate outside Australia;
- Complete a transaction, such as an International Money Transfer; or
- Comply with laws and assist government or law enforcement agencies.

BFS does not collect sensitive information (such as information about your religion, ethnicity or health). If we need this type of information, we'll ask for your permission – except where otherwise allowed by law.

Wherever lawful and practicable, individuals may deal anonymously with BFS but given the nature of BFS' services, it is unlikely that this will be a viable option. BFS does not use official identifiers (e.g. tax file numbers) to identify individuals. An individual's name or Australian Business Number is not an identifier for the purposes of the Privacy Act and hence may be used to identify individuals.

15 QUALITY OF PERSONAL INFORMATION

BFS takes all reasonable steps to ensure the personal information held about individuals is accurate, up-to-date and complete. BFS will verify personal information at the point of collection. The accuracy of records is also maintained by regular mail-out of statements and the periodic roll-over of commercial loans.

BFS encourage clients to tell BFS immediately if they change their contact details (such as phone number, street address or email address) or if any of their details need to be corrected or updated. A person wishing to update their personal information may contact our staff or the Privacy Officer on the contact details shown within this document.

16 ACCESS TO PERSONAL INFORMATION

Where a person requests access to their personal information, BFS' policy is, subject to certain conditions (as outlined below) to permit access. BFS will correct personal information where that information is found to be inaccurate, incomplete or out of date. BFS will not charge an individual for reasonable access and correction requests. If a person wishes to access their personal information or correct it, they should contact the Privacy Officer, and BFS will seek to provide such information within a reasonable period of time, and in the manner so requested (where reasonable to do so).

BFS may not always be able to give a client access to all the personal information BFS holds about them. If this is the case, BFS will provide a written explanation of the reasons for such a refusal, together with details of the complaints process if clients wish to challenge the decision.

BFS may not be able to give client access to information in the following circumstances:

- Where BFS reasonably believe this may pose a serious threat to the life, health or safety of any individual or to public health/safety;
- Which would unreasonably impact the privacy of another individual;
- Where such request is reasonably considered to be frivolous or vexatious;
- Which relates to existing or anticipated legal proceedings which would otherwise not be accessible in the discovery process relating to such proceedings;
- Which would reveal BFS' intentions and thereby prejudice negotiations with a client;
- Which would be unlawful;
- Which is prohibited by law or a court/tribunal order;
- Which relates to suspected unlawful activity or serious misconduct, where access would likely prejudice the taking of appropriate action in relation thereto;
- Where enforcement activities conducted by or on behalf of an enforcement body may be prejudiced; or
- Where access would reveal details regarding a commercially sensitive decision-making process.

17 CORRECTION OF PERSONAL INFORMATION

Where BFS believes information held about an individual is inaccurate, out-of-date, incomplete, irrelevant or misleading, OR an individual requests the correction of information held about them, BFS will take all reasonable steps to correct such information in a reasonable time frame. No fees are payable for such requests. If a client requests us to similarly advise a relevant third party of such correction, BFS will facilitate that notification unless impracticable or unlawful for us to do so.

If BFS intends to refuse to comply with a correction request, BFS will notify the client in writing of reasons for such a refusal, and the complaints process they may avail themselves of if they wish to challenge that decision. A client may also request that BFS associate the personal information the organisation hold with a statement regarding their view of its inaccuracy.

18 SECURITY OF PERSONAL INFORMATION

BFS will take reasonable steps and precautions to keep personal information secure from loss, misuse, and interference, and from unauthorised access, modification or disclosure.

Personal information in hard copy is stored in BFS State offices and offsite storage facilities. Personal information imaged and stored on electronic databases requires password access and access is restricted to authorised personnel. The BFS legal advisers also store some personal information and BFS is assured that their premises and the information stored by them are secure.

Where information is no longer required to be held or retained by BFS for any purpose or legal obligation, BFS will take all reasonable steps to destroy or de-identify the information accordingly.

19 PRIVACY COMPLAINTS

If a client has a complaint relating to BFS' compliance with privacy laws or the treatment of personal information, they should contact BFS' Privacy Officer on Ph: 1300 650 542. The Privacy Officer will investigate the complaint and endeavour to resolve the issue to the client's satisfaction. If the client is not satisfied with the outcome of the complaint, they have the right to lodge a complaint with the Office of the Australian Information Commissioner by telephoning 1300 363 992 or visiting their website at www.oaic.gov.au.

20 NOTIFIABLE DATA BREACH SCHEME

The Privacy Amendment (Notification of Data Breaches) Act 2017 ("NDB scheme") came into effect from 23 February 2018.

The NDB scheme applies to BFS and BFS has an ongoing obligation to take reasonable steps to handle personal information in accordance with Australian Privacy Principles. This includes protecting personal information from misuse, interference and loss, and from unauthorized access, modification and disclosure.

The Office of the Australian Information Commission (OAIC) is the key regulator responsible for functions that are conferred by the Privacy Act. OAIC has issued a summary fact sheet outlining the application of the NDB scheme. Headings used therein are adopted herein and some content has been replicated to explain the application of the NDB scheme to BFS.

The NDB scheme imposes mandatory reporting requirements on BFS when collecting personal information, including such things as identity details, residency, financial and transaction information, credit reports, credit eligibility or TFNs. The fundamental purpose of the NDB scheme is to allow customers to undertake corrective procedures in circumstances when their personal information has been compromised.

20.1 SUSPECTED OR KNOWN DATA BREACH

A data breach is unauthorised access to or unauthorised disclosure of personal information, or loss of personal information, that an entity holds. BFS employees are required to immediately record a data breach on the BFS Incident Report and simultaneously notify the Privacy Officer.

20.2 CONTAIN

BFS is required and will undertake, to first contain a suspected or known data breach and take immediate steps to limit any further access or distribution of the affected personal information, or other possible compromise of other information.

20.3 ASSESS

BFS will next undertake an assessment of the data breach. The NDB scheme is intended to capture "eligible" data breaches. BFS will create a procedure to conduct an assessment and will follow OAIC's suggested three-stage process, namely Initiate, Investigate and Evaluate to identify an eligible data breach. The Privacy Officer will lead and take responsibility for this assessment and in doing so will apply the criteria below:

An "eligible data breach" is deemed to have occurred if either:

- unauthorised access to, or disclosure of, the relevant information, and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or
- the relevant information is lost in circumstances where unauthorised access to or unauthorised disclosure of that information might occur, and if it did, a reasonable person would conclude that it would be likely to result in serious harm to any of the individuals to whom the information relates.

The Privacy Officer, in undertaking this assessment, should also consider remedial action. The assessment should be expeditious and, generally, within 30 days and should be documented.

20.4 NOTIFY

Where serious harm is likely, BFS must prepare a statement for the OAIC Commissioner that contains:

- BFS' identity and contact details
- A description of the breach
- The kind/s of information concerned
- How BFS will respond to the breach
- Recommended steps for individuals

BFS must also notify affected individuals and inform them of the content of the statement.

There are three options for notifying:

1. Notify all individuals

2. Notify only those individuals at risk of serious harm

If neither of these options are practicable, then:

BFS can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

Notification exceptions can apply to the mandatory reporting obligations. The most notable exception is if BFS has taken necessary remedial actions upon discovering a data breach before serious harm has occurred. In this instance, BFS is not required to report the breach to the OAIC or to affected individuals.

20.5 REVIEW

BFS will implement a review process after or during the relevant assessment by the Privacy Officer. The Privacy Officer will take the lead in the process and review the incident and take action to prevent future breaches. These preventative actions may include:

- Investigate and understand the cause of the breach
- Develop a prevention plan
- Conduct audits to ensure the prevention plan is implemented and being adhered to
- Update relevant policies and procedures and practices, including frequency and nature of staff training.

BFS will also consider whether to report the incident to other relevant bodies.

21 CONTACT INFORMATION

Baptist Financial Services Australia Ltd. Phone: 1300 650 542

BFS' Privacy Officer on Phone: 1300 650 542