Privacy Policy

bobby goldsmith foundation
practical emotional financial support

Document Status	Final
Version	1.3
Short Description	Privacy Policy
Relevance	To all clients, staff, volunteers and Board Members of BGF
Approval	Endorsed by CEO, ratified by Risk and Audit Committee, Approved by BGF Board
Policy Owner	CEO
Policy Contact	Andrew Buchanan
Date Implemented	19/02/18 following approval
Date Amended	[day/month/year] following approval of amendments
Scheduled review date	February 2019

Version Control Panel

Version #	*Date Issued*	*Date Reviewed*	*Reason for Review*	*Reviewed By*	*Comments*
1.1	April 2014	April 2014	Section missing from Public Health Act 1991	Andrew Buchanan	Section 10.5 amended to reflect Act.
1.2	May 2014	May 2014	Inclusion of *Health Records and Information Privacy Act (NSW) 2002* provisions	Andrew Buchanan	Client access to information retained on them
1.3	February 2018	February 2018	Introduction of Privacy Amendment (Notifiable Data Breaches) Bill 2016 – refer Section 10	Andrew Buchanan	Mandatory data breach reporting

1. CONTEXT
   1.1 As the Bobby Goldsmith Foundation (BGF) is an organisation that collects personal and sensitive information, the 13 Australian Privacy Principles apply to it.
   1.2 BGF remains deeply committed to respecting and upholding privacy protection under the Privacy Act.
   1.3 Among other requirements, the APPs regulate how we collect, use, disclose and retain personal information.

2. GUIDING PRINCIPLES
   2.1 Protection of an individual's right to privacy regarding their personal information.
   2.2 Respect for the personal information of an individual.

3. PURPOSE
   3.1 This document is Bobby Goldsmith Foundation's (BGF's) policy on Privacy.
   3.2 The objectives of BGF's Privacy Policy are:
      - To ensure that BGF takes seriously the responsibility attached to gathering and maintaining sensitive client, donor and contractor information;
      - To ensure that BGF has satisfactory systems and procedures in place to handle and protect personal information; and
      - To outline BGF's approach to handling privacy complaints.

4. SCOPE
   4.1 This document applies to the personal information held by BGF.
   4.2 Should at any time you provide us with personal information about someone other than yourself, you must vouch that you have received consent from the person so identified to provide such information.

5. REFERENCES
   5.1 Privacy Act 1988
   5.2 Privacy Amendment (Enhancing Privacy Protection) Act 2012 [that identifies the 13 new Australian Privacy Principles (see Attachment)]
   5.3 Privacy Amendment (Notifiable Data Breaches) Bill 2016
   5.4 Public Health Act 1991 (NSW)
   5.5 Health Records and Information Policy (NSW) 2002 (HRIPA)
   5.6 BGF Confidentiality Agreement
   5.7 BGF Code of Conduct
   5.8 BGF Records Management Policy

6. DEFINITIONS
   6.1 'Personal Information' means information, or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

6.2 'Sensitive Information' means:

a. Information, or an opinion, about an individual's:
   - Racial or ethnic origin; or
   - Political opinions; or
   - Membership of a political association; or
   - Religious beliefs or associations; or
   - Philosophical beliefs; or
   - Membership of a professional or trade association; or
   - Membership of a trade union; or
   - Sexual preferences or practices; or
   - Criminal record (that is also personal information); or

b. Health information about an individual; or

c. Genetic information about an individual that is not otherwise health information

Source: Privacy Act 1988 – Section 6 - Interpretation

7. RESPONSIBILITIES

7.1 The CEO has overall responsibility for compliance with the implementation of Privacy Act including the Australian Privacy Principles across the organisation.

7.2 Each member of the BGF Board, staff member, volunteer or contractor has individual responsibility for upholding BGF's commitment to privacy as espoused through its Privacy Policy and as managed and complied with through the various systems and mechanisms in place.

7.3 Each member of staff, volunteer and Board Member has signed a Confidentiality Agreement as well as agreeing to abide by BGF's Code of Conduct.

8. COMMUNICATION

8.1 Following approval, the policy will be implemented (published).

8.2 The policy will be placed in the BGF Policy Bank.

8.3 All BGF personnel (staff, volunteers and Board members) will read the policy and sign a pro-forma document to acknowledge their understanding of the policy and their commitment to ensuring it is complied with at all times.

8.4 Hard copy version of the Privacy Policy to be printed and made available upon request.

9. PERSONAL INFORMATION

9.1 The types of information we collect are typically, not exclusively,:
   - Identity Information such as name, date of birth, gender etc.;
   - Contact Information eg address, phone number, email address etc.;
   - Health and Medical Information, typically of a highly sensitive nature (refer to Section 11 – Sensitive Information);
   - Financial Information about financial affairs including bank account and credit card details, transactional values, asset and liability positions, TFN, etc.;
   - Statistical Information such as online behaviour, thoughts, views and ratings of certain services etc.;

- We acknowledge that some of the information we collect is of a highly sensitive nature, and will limit the collection of this type of information to that which is necessary to enable us to better perform our services (refer Section 11 specifically).

9.2 The sources of information are:

- Clients of our services;
- Staff, volunteers and Board members of BGF;
- Donors;
- Suppliers and contractors;
- Other health service providers;
- Research databases; and
- Research participants.

9.3 Information is collected in the following ways:

- Directly from the individual, either in person ie. face-to-face, via the telephone, via an email, online, via a questionnaire, or via a response device from direct marketing activity;
- Via third parties such as contractors, health care workers, social workers. Should we receive personal information from a third party and we suspect relevant consent has not been provided, we will attempt to contact the individual to ensure they are aware of our having being given this information, and confirming their approval of our retaining it. Should this not be approved, the information will be destroyed; and
- BGF will not gather personal information in an unlawful manner, or in a way which is considered intrusive or harassing.

9.4 The primary purposes for collecting personal information are:

- To verify identity upon commencement of an occasion of service;
- To provide BGF's primary functions and activities;
- To better understand communication preferences so that we can provide appropriate information and services in the manner and mode preferred;
- To process financial donations and provide receipts;
- To maintain an accurate history of an individual's ongoing relationship with the organisation;
- To accurately target and communicate our services, support, donations, campaigns, research programs;
- To enable support through volunteering, donations, in-kind;
- To evaluate our programs and services for continuous improvement;
- To enable us to measure the impact our programs are having, and report this information back to our donors and funders; and
- To comply with relevant legislation.

9.6. Use of personal information for secondary purposes

- Use or disclosure of personal information for secondary purposes is permitted only if:
  - The secondary purpose is related to the primary purpose for collection;

- For sensitive information (see Section 11 below), the secondary purpose is directly related to the primary purpose; and
- The individual would reasonably expect BGF to use or disclose the information for the secondary purpose.

9.6 De-Identification of Personal Information

- Records maintained by us will be attached to an individual's personal identity however where information is aggregated for evaluation or research purposes, this data may be de-identified; and

9.7 Government Related Identifiers

- BGF will not adopt a government related identifier of an individual as its own identifier of the individual.

10. NOTIFIABLE DATA BREACHES

10.1 Overview

- An amendment to the Privacy Act will become law on 22 February 2018. This bill, known as the Privacy Amendment (Notifiable Data Breaches) Bill 2016 will require all government agencies and organisations regulated by the Privacy Act to provide notice to the Australian Information Commissioner and affected individuals of an eligible data breach.

10.2 What is an eligible data breach?

- An eligible data breach happens if:
  (a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
  (b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
- An entity must make a notification if:
  (a) it has reasonable grounds to believe that an eligible data breach has occurred; or
  (b) it is directed to do so by the Commissioner.
- Serious harm could include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.
- In deciding whether there is an eligible data breach, entities are required to have regard to a list of 'relevant matters' included in the Bill. It is not intended that every data breach be subject to a notification requirement.

10.3 Suspected eligible data breach

- If an entity is aware that there are reasonable grounds to suspect that there may have been an eligible data breach of the entity, the entity must:
  (a) carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and

(b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity suspects there may have been a breach.

10.4 How is a notification given?

- In the event of an eligible data breach, an entity is required to notify the Commissioner and affected individuals as soon as practicable after the entity is aware that there are reasonable grounds to believe that there has been an eligible data breach (unless an exception applies, see below). The notification must include:
    - the identity and contact details of the entity
    - a description of the data breach
    - the kinds of information concerned, and
    - recommendations about the steps that individuals should take in response to the data breach.
- In providing the information described above to affected individuals, the entity also has discretion to notify either each affected individual or, if not all affected individuals are deemed to be 'at risk' from an eligible data breach, only those affected individuals who are deemed to be at risk.

10.5 Exceptions

- There may be circumstances in which it is impracticable to provide a notification to affected individuals, either collectively or only to those at risk. The Bill provides that, in these circumstances, an entity will not be required to provide notice directly to each affected individual but will rather be required to provide the information described above on its website (if any) and to take reasonable steps to publicise the information. There is no obligation to give a notification where entities have taken remedial action following an eligible data breach or potential eligible data breach and a reasonable person would conclude that, as a result of the remedial action, the unauthorised access or unauthorised disclosure of personal information (including an unauthorised access or unauthorised disclosure following loss of the information) is not likely to result in serious harm to the affected individuals. In addition, the Commissioner may exempt an entity from providing notification of an eligible data breach where the Commissioner is satisfied that it is reasonable in the circumstances to do so, having had regard to several matters prescribed in the Bill.

11. SENSITIVE INFORMATION

11.1 Under APP 3, sensitive information cannot usually be collected without the person's consent. Information about a person's health is considered one type of sensitive information.

11.2 APP 3 also permits organisations to collect health information without consent in certain circumstances, where the information is collected for:

- Research, or the compilation or analysis of statistics relevant to public health and public safety; and
- The management, funding or monitoring of a health service.

11.3 Typically but not exclusively, sensitive information can include information or an opinion about an individuals' HIV status, political beliefs, political and professional/trade associations, sexual preferences, the existence or not of a criminal record, ethnicity and of course information about health.

11.4 BGF is fully cognisant of its requirements under the Public Health Act 1991 (NSW) which provides that a person who, in the course of providing a service, acquires information that another person: (a) has been, or is required to be, or is to be, tested for HIV, or (b) is, or has been, infected with HIV, must take all reasonable steps to prevent disclosure of the information to another person. Breach of this provision is a criminal offence punishable by a fine of up to $5,500.

12. DIRECT MARKETING

12.1 From time to time BGF could undertake direct marketing activities to individuals, based on personal information we have received. In all instances, the individual should receive an opportunity to opt-out of receiving such communication in the future. **Opt-out** notices will be clearly and conspicuously identified on all direct marketing materials. Should an individual choose not to opt-out, BGF will assume that they are providing us with consent to continue direct marketing into the future.

12.2 Additionally, BGF provides recipients of all emails with the opportunity to 'Unsubscribe'.

12.3 BGF does not sell, rent, or generally make available personal information to any third parties for the purposes of marketing solicitations.

13. DISCLOSURE TO THIRD PARTIES

13.1 From time to time, it may be necessary for BGF to disclose personal information to others. This could be in order to perform our duties, or it may be in order for an individual to receive services from other service providers. Examples of such third party disclosure include:

- Other health support agencies;
- Other professional services e.g. legal services, accounting services etc.;
- Law enforcement agencies e.g. the police;
- Service providers e.g. printers; and
- Researchers.

These third parties will have access to personal information to the extent needed to perform their functions or as required by law but may not use it for other purposes.

13.2 Whenever we plan to disclose personal information we will ensure that the individual has provided us with the appropriate consent to do so.

13.3 There may be circumstances when we are obliged to disclose personal information about an individual without their consent. Such circumstances include:

- When we are required to by law;
- When a minor is perceived to be at risk;
- When it's in the interests of public health or safety; and

- When it's in the interests of personal health or safety.

13.4 Should an individual have a guardian appointed to care for their affairs, it may be necessary for us to disclose their personal information to this person.

14. CROSS-BORDER DISCLOSURE

14.1 Currently BGF avails itself of an outsourced online, financial accounting service (Xero) that stores our data beyond our borders (in the US).

14.2 While personal information will be stored on servers located in the U.S., it will remain within Xero's effective control at all times. Each data hosting provider's role is limited to providing a hosting and storage service to Xero, and steps have been taken to ensure that the data hosting providers do not have access to, and use the necessary level of protection for, our personal information. These hosting providers do not control, and are not permitted to access or use your personal information, except for the limited purpose of storing the information. This means that, **for the purposes of Australian privacy legislation and Australian users, Xero does not currently "disclose" personal information to third parties located overseas**.

15. PERSONAL INFORMATION STORAGE

15.1 In keeping with APP 11, BGF takes all reasonable steps to protect personal information in its possession from misuse, interference and loss, and from unauthorised access, modification or disclosure.

15.2 Client's personal information is stored in both hard copy format and electronically. Storage is managed via our Records Management Policy and Procedures.

15.3 Hard copies of client's files are created, maintained and stored on site within BGF's main offices in Devonshire Street, Sydney NSW. Files are housed within a lockable compactus in an area where access is limited to staff and volunteers.

15.4 Archived files of lapsed and deceased clients are stored offsite for up to 7 years as required by law. Storage is undertaken by a third party provider who is compliant with the Australian Privacy Principles. We are however unable to guarantee any unauthorised or unlawful access to the information stored offsite, and as such are not liable for any such access.

15.5 Electronic data storage is via BGF's password-protected relational database. A daily (nightly) back-up of electronically written data is performed and sent offsite as part of BGF's Disaster Recovery Plan.

15.6 All decommissioned servers and hardware including PCs are sent offsite to a recycling centre for destruction/recycling. They contain no data when dispatched offsite.

15.7 Personal information remains attached to an electronic file record until such time as the record is deleted (on request) or upon our purging the database after 7 years of ongoing inactivity.

15.8 Donor's personal information is stored both in hard copy format and electronically. Storage is managed via our Records Management Policy and Procedures

15.9 Hard copies of personal information encompass establishing a donor relationship with BGF. Such documents are stored on-site for up to 7 years being the statutory requirement.

15.10 Electronic storage of donor information occurs on Raiser's Edge, an electronic donor database that is operated in-house.

15.11 Electronic records written to Raiser's Edge daily are backed up each night and stored offsite as part of BGF's Disaster Recovery Plan.

15.12 Should an individual become aware of any misuse, interference or loss of personal information, or unauthorised access to their personal information, they should notify us at their earliest opportunity.

16. YOUR PERSONAL FINANCIAL INFORMATION

16.1 Any credit card or debit card numbers, expiry dates and CCVs we receive in the course of receiving a donation to BGF are processed using SSL certificates via a third-party financial services provider. SSL (secure socket layer) technology is the current industry standard for processing online payments, and as such, precludes any unlawful third party from unauthorised access to this information

16.2 On our servers, this data remains encrypted, and thus inaccessible to all except authorised BGF staff.

16.3 Personal financial information received from clients is stored both in hard copy format within the client's file, and electronically attached to the client record within the client database.

17. ACCESSING PERSONAL INFORMATION

This section is informed by the HRIPA. The HRIPA applies to organisations, BGF being defined as a 'private sector person'.

17.1 Individuals have the right to access the personal information we retain about them. Should they wish to gain access to this information, we require that they apply in writing, following our guidelines (see Attachment), specifying what information they wish to receive, and why.

17.2 We are however not obliged to provide access to this information in certain circumstances, as follows:

- Where gaining access would pose a serious risk to the life, safety or health of any individual, to public health or to public safety. This refusal must be done in accordance with any guidelines issued by the NSW Privacy Commissioner, however to date there do not appear to be guidelines published to make for sufficient grounds to deny access. The individual must be notified should this be the case so that they can request that information be provided to a nominated registered medical practitioner;
- Where gaining access would impinge on the safety and privacy of others;
- Where gaining access is unlawful or prejudicial to ongoing legal proceedings, negotiations or enforcement activity;
- Where we are obliged via a pre-existing order to deny access;

- Where we consider such a request to be trivial, or vexatious, or of a repeated nature and the individual has been provided with access the health information previously; and
- Where the request for access is of a kind that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again.

17.3 Where we choose not to allow access to the information we hold about an individual, we are obliged, in accordance with HRIPA guidelines, to explain the reason/s why.

17.4 Should we become aware of any unauthorised access to an individual's personal information, we will contact them at our earliest opportunity, subsequent to our having investigated when and how the unauthorised access took place, and what information was accessed.

18. UPDATING PERSONAL INFORMATION

18.1 Individuals may request that BGF update, modify or delete any personal information that we currently hold on them.

18.2 Before proceeding with the request we will ensure that their identity is verified.

18.3 Where we believe the information we hold is inaccurate or out-of-date, we have the right to correct it.

18.4 To request access to their personal information, or to request an update to their personal information, an individual may contact us in a number of ways:

- By mail to BGF, PO Box 1444, Strawberry Hills, NSW 2012
- By email to bgf@bgf.org.au
- By telephone at 02 9283 8666
- By fax to 02 9283 8732
- Online at www.bgf.org.au

19. COMPLAINTS ABOUT BGF'S HANDLING OF PERSONAL INFORMATION AND BGF'S PRIVACYPOLICY

19.1 BGF operates a Privacy Complaint Handling process (mechanism) that guides the approach to take should an individual have any questions or complaints.

19.2 Individuals should refer to the attached guidelines when lodging a complaint.

20. BGF'S COMPLIANCE PROGRAM

20.1 A Compliance Program has been established to meet our obligations for the open and transparent management of personal information as required under APP 1 (refer to Annexure A)

20.2 The program has 3 main components, namely:

- Training
- Complaints Handling
- Risk and Audit Committee

21. ACCESSING BGF's PRIVACY POLICY

21.1 A copy of our Privacy Policy is available upon request. Alternatively you can download a copy of our Privacy Policy from the BGF website (www.bgf.org.au).

21.2 From time to time, we will review this policy and make amendments. These amendments will be reflected in the latest version of our policy.

ATTACHMENTS

1. The Australian Privacy Principles
2. Guidelines for Requesting Access to your Personal Information
3. Guidelines for Handling a Privacy Complaint

ATTACHMENT #1

The Australian Privacy Principles

Effective 12 March 2014, the Australian Privacy Principles (APPs) will replace the National Privacy Principles and the Information Privacy Principles and will apply to organisations, and Australian Government (and Norfolk Island Government) agencies.

The privacy fact sheet below provides the text of the 13 APPs from Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which amends the *Privacy Act 1988*.

The link below will take you to a series of fact sheets on the 13 new Privacy Principles.

http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-17-australian-privacy-principles_2.pdf

The Privacy Commissioner's website can be located at www.privacy.gov.au. There you can find detailed information on the privacy obligations of organisations. You will also find a copy of the Privacy Act.

ATTACHMENT #2

Guidelines for Requesting Access to Personal Information

1. The request MUST be made in writing to BGF.
2. The request must state the name and address of the individual making the request.
3. The specific health information to which access is being sought must be sufficiently identified.
4. The form (manner) in which the individual wishes to receive the information must be provided (under the HRIPA provisions).
5. Receipt of the request will be acknowledged within 3 working days of our receiving it, and BGF must respond to the request within 45 days of receiving it.
6. BGF must be reasonably satisfied of the person's authority to access the information and can therefore request evidence of their identity.
7. Where a request is made to view or inspect what data is held on the system about the individual, an appointment will need to be made.
8. Where the request is for information to be corrected, updated or deleted, the individual should state clearly what piece or pieces of information are affected, and what the proposed changes are.
9. BGF does not provide online access to view or update client data.

Address all requests in writing to:

Bobby Goldsmith Foundation

P O Box 1444

Strawberry Hills

NSW 2012

Or email bgf@bgf.org.au

For support or to ask any questions about accessing your personal information, call 02 9283 8666 during normal business hours, Monday to Friday.

ATTACHMENT #3

Guidelines for Handling a Privacy Complaint

1. A complaint MUST be made in writing to BGF.
2. Receipt of the complaint should be acknowledged with 3 working days of our receiving it.
3. The complaint should be given to the Manager of the relevant business area to which the complaint pertains.
4. The Manager will assess the complaint and, if necessary, investigate the circumstances surrounding it.
5. Following discussions with the CEO, a written response will be sent to the individual, usually within 10 working days of receipt of the original complaint.
6. If the response is considered unsatisfactory in any way, the individual may approach the Australian Information (Privacy) Commissioner to request independent arbitration or conciliation.

Address all complaints in writing to:

Bobby Goldsmith Foundation

P O Box 1444

Strawberry Hills

NSW 2012

Or email bgf@bgf.org.au

1. For support or should you have any questions about BGF's Privacy Complaint Handling Process, call 02 9283 8666 during normal business hours, Monday to Friday.

ANNEXURE A

PRIVACY ACT COMPLIANCE PROGRAM

Bobby Goldsmith Foundation (BGF) has established a Privacy Act Compliance Program (**Compliance Program**) in response to Australian Privacy Principle 1 – Open and Transparent Management of Personal Information. The program aims to comply with each of the following requirements:

1. Training

1.1. Privacy policy guidelines, which must be observed by all BGF staff and volunteers in relation to the collection, use, storage, security and disclosure of personal information, sensitive information and health records will form the basis of a training program, to be undertaken as follows:

1.1.1. For existing staff and volunteers:	Within 2 months of the implementation of the new Australian privacy principles, and subsequently updated every 2 years;
1.1.2. For new staff and volunteers:	As part of their induction training
1.1.3. For Board members:	(TBC in consultation with David and Damien)

1.2. BGF will ensure that the training referred to in paragraph 1.1 above is administered by a suitably qualified trainer with expertise and experience in Privacy law and compliance.

2. Complaints Handling

2.1. BGF has:

2.1.1. developed procedures for recording, storing and responding to Privacy Act complaints; and

2.1.2. developed a complaint handling mechanism.

3. Risk and Audit Committee

3.1. BGF will place Privacy Act issues on the agenda of its bi-monthly Risk and Audit Committee meetings.

3.2. Any identified breaches of privacy, whether emanating through the complaint handling process or not, will be discussed and remedies sought for implementation.

3.3. Privacy matters will be reported on in the annual report of the Risk and Audit Chairman.

4. If requested by the Office of the Australian Information Commissioner, BGF will provide, at its own expense, copies of any other documents or information in respect of matters which are the subject of the Compliance Program.