Internal Privacy and Procedure Policy

Entity: Integrity Financial Planners Pty Ltd **(IFP)**

ABN: 71 069 537 855

AFSL: 225051

Contents

Intellectual Property and disclaimer

Version 1.0 – December 2020

References:

- Privacy Act 1988
- Australian Privacy Principles Guidelines

1. Background and purpose of document

1.1 Background

Integrity Financial Planners Pty Ltd ("IFP") provides financial services to clients and as a result discloses information about its clients to third parties (e.g. financial institutions, insurers and fund managers) for a benefit, service or advantage. IFP is also a reporting entity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Therefore, IFP is required to comply with its obligations under the Privacy Act 1988, the Australian Privacy Principles ("APP").

As a registered tax (financial) adviser licensee, IFP is also required to comply with Item 6 of the Code of Professional Conduct outlined in section 30.10 of the Tax Agent Services Act 2009 ("Code").

The Internal Privacy Policy ("Policy") addresses IFP's policy on the management of client information, including how IFP deals with a notifiable data breach.

1.2 Purpose and framework

This policy (**Policy**) is developed by the Licensee for the purposes of enabling the Licensee to:

1.2.1 meet its obligations under the Corporations Act and ASIC guidance; and

1.2.2 This policy (**Policy**), in conjunction with other policies, has been developed by IFP (**Licensee**) for the purposes of enabling the Licensee to meet its obligations under the Act and ASIC guidance.

1.3 Responsibility

1.3.1 The Responsible Manager/s (or a delegate with appropriate experience and seniority) will be responsible for ensuring that the Licensee:

(i) meets the requirements of this Policy;

(ii) considers and assesses the risks faced by the Licensee when carrying on a financial services business;

(iii) reviews this Policy on not less than an annual basis (unless more immediate updates are required due to legislative or regulatory change).

2. Policy Statement

IFP will comply with its obligations under the 13 APP:

(a) APP 1 - Open and transparent management of personal information;

(b) APP 2 - Anonymity and pseudonymity;

(c) APP 3 - Collection of solicited personal information;

(d) APP 4 - Dealing with unsolicited personal information;

(e) APP 5 - Notification of the collection of personal information;

(f) APP 6 - Use or disclosure of personal information;

(g) APP 7 - Direct marketing;

(h) APP 8 - Cross-border disclosure of personal information;

(i) APP 9 - Adoption, use or disclosure of government related identifiers;

(j) APP 10 - Quality of personal information;

(k) APP 11 - Security of personal information;

(l) APP 12 - Access to personal information; and

(m) APP 13 - Correction of personal information.

IFP will also comply with its obligations under Part IIIC of the Privacy Act 1988 to notify the Australian Information Commissioner ("**Commissioner**") and affected individuals of eligible data breaches.

IFP will not disclose any information relating to a client's affairs to a third party without the client's permission: Item 6 of the Code.

2.1 APP 1 – Open and transparent management of personal information

IFP has a clearly expressed and up-to-date Privacy Policy regarding the management of personal information. This Privacy Policy is available on IFP's website or available upon request.

The Privacy Policy is reviewed on not less than an annual basis by IFP to ensure it remains current. The Privacy Policy is supplemented by this Policy.

2.2 APP 2 - Anonymity and pseudonymity

It is impracticable for IFP to deal with individuals who have not identified themselves or who have used a pseudonym. IFP only allows individuals not to be identified, or to use a pseudonym, when requesting publicly available information; e.g. requesting for IFP's postal address.

2.3 APP 3 - Collection of solicited personal information

IFP collects personal information for the primary purpose of providing financial services to those persons. The collection of personal information is required for IFP to comply with certain obligations under the Corporations Act 2001. Personal information may also be used for secondary purposes listed in section 2.6 below.

Personal information is collected where it is reasonably necessary for IFP's functions or activities. IFP will only collect sensitive information with the individual's consent.

2.4 APP 4 - Dealing with unsolicited personal information

If IFP receives unsolicited personal information about an individual, IFP will consider whether it could have collected the information if IFP requested the information from the individual. If not, IFP will destroy the information or ensure the information is de-identified. Otherwise, IFP may retain the personal information as long as APP 5 to 13 have been complied with.

2.5 APP 5 - Notification of the collection of personal information

IFP typically collects personal information directly from the individual or from third parties. IFP will only collect information about an individual from a third party (e.g. financial institution, insurer or superannuation provider) after seeking the individual's consent. IFP notifies the individual about matters relating to the collection of personal information via its Privacy Policy.

2.6 APP 6 - Use or disclosure of personal information

IFP uses or discloses information about an individual for the primary purpose of providing the individual with financial services and tax (financial) services. IFP may also use or disclose information about an individual for the secondary purpose of:

- attempting to identify other products and services that may be of interest to the individual;
- referring the individual to a suitable professional to assist the client with other services (e.g. accounting, legal services etc);
- conducting any professional quality control review program; and
- managing our business operations such as maintaining secure IT systems.

IFP can use or disclose information for a secondary purpose where:

- the individual has consented to the use or disclosure of the information; or
- the individual would reasonably expect IFP to use or disclose the information for the secondary purpose and the secondary purpose is related to the primary purpose. If the information is sensitive information, the secondary purpose must be directly related to the primary purpose.

2.7 APP 7 - Direct marketing

IFP can only use personal information (other than sensitive information) for direct marketing purposes when:

- IFP collected the information from the individual;
- the individual would reasonably expect IFP to use or disclose the information for direct marketing;
- IFP provides a simple means by which the individual may easily opt-out of receiving direct marketing communications from IFP; and
- the individual has not made an opt-out request to IFP.

Sensitive information can only be used or disclosed for direct marketing purposes when the individual has consented to it.

2.8 APP 8 - Cross-border disclosure of personal information

IFP may disclose personal information about an individual to a person who is not in the Australian jurisdiction by using administrative services or cloud-based servers overseas. Where it does, IFP will ensure that it has complied with one of the following requirements:

- taken reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information by entering into a contractual agreement with the overseas recipient that requires the overseas recipient to comply with the APPs, other than APP 1;
- IFP reasonably believes that the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the personal information in a way that, overall, is at least substantially similar to the way in which the APP protect the information and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
- IFP expressly informs the individual and the individual consents to his/her personal information to be used or disclosed overseas.

2.9 APP 9 - Adoption, use or disclosure of government related identifiers

IFP does not adopt a government related identifier of an individual as its own identifier. IFP can use or disclose an individual's government related identifier (e.g. TFN) where the individual has consented to it.

Refer to Appendix A for the Authority to Collect, Use and Disclose TFN Form.

2.10 APP 10 - Quality of personal information

IFP will take reasonable steps to ensure that the personal information collected is accurate, up-to-date and complete. Personal information collected by IFP is typically summarised in a fact find, proposal, schedule of insurance or Statement of Advice. The individual confirms the completeness and accuracy of the personal information in writing or by signing a relevant document eg Fact Find, Authority to Proceed, Insurance application, proposal document, offer document etc.

2.11 APP 11 - Security of personal information

IFP takes the following steps to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure:

- password protection on computers and servers;
- ensuring access to client's personal information is password protected and/or two-factor authentication is used;
- ensuring that passwords are used when accessing third party websites (e.g. access to platforms and bank accounts);
- ensuring that any hard copy documents with client identifiers are retained and stored in a secure location eg locked drawer or cabinet, storage facility etc.
- ensuring that passwords are not shared with third parties;

IFP is required to hold records in relation to provision of personal advice to retail clients for 7 years after the day the client is recorded as no longer being a client. When IFP no longer needs the information, IFP will take reasonable steps to destroy the information or to ensure that the information is de-identified.

2.12 APP 12 - Access to personal information

If IFP receives a request from an individual to provide access to their personal information, IFP may seek advice from its legal counsel or relevant compliance resource, prior to the provision of that information. Where IFP provides a person with access to that person's personal information it will do so within a reasonable period after the request is made ie up to 30 days as per the IFP Privacy Policy.

Request to access the personal information can be refused if:

- IFP reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between IFP and the individual, and would not be accessible by the process of discovery in those proceedings;

- giving access would reveal the intentions of IFP in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order;
- both of the following apply:
    - IFP has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to IFP's functions or activities has been, is being or may be engaged in;
    - giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

If IFP refuses to provide access to the personal information, IFP can take reasonable steps to give access in a way that meets the needs of IFP and the individual. IFP will ensure that any fee charged for access to the personal information is not excessive.

Where IFP refuses to give access to the personal information, or to give access in the manner requested by the individual, IFP will give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal.

2.13 APP 13 - Correction of personal information.

IFP will take reasonable steps to ensure that the personal information collected, used or disclosed is accurate, up-to-date, complete and relevant. IFP will also amend the personal information about the individual if the individual notifies IFP of any error.

If IFP refuses to correct the personal information as requested by the individual, IFP will give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal.

IFP will respond to the request for correction of personal information within a reasonable period after the request is made and will not charge the individual for the making of the request or for correcting the personal information.

2.14 Notification of eligible data breaches

IFP will notify the Commissioner and affected individuals of an eligible data breach, which is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in IFP's position.

Refer to IFP's Data Breach Response Plan for further details.

2.15 Compliance with the Code

IFP is a registered tax (financial) adviser Licensee and is required to comply with Item 6 of the Code. IFP will seek confirmation from a client prior to disclosing any information relating to a client's affairs to a relevant third party.

A relevant third party includes IFP's professional advisers, technical services teams (such as paraplanners), auditors, contractors, IT specialists, offsite data storage services (including 'cloud storage') and others that assist IFP with the provision of financial services and financial products to the client.

IFP will require its clients to sign a Privacy Confirmation form as part of IFP's Fact Find.

3 Commitment

The Compliance Manager is responsible for ensuring that the IFP Privacy Policy is up-to-date and is reviewed on a not less than annual basis.

The Compliance Manager is also responsible for reporting eligible data breaches to the Office of the Australian Information Commissioner and affected individuals.

4 Authorised Representative Requirements

Authorised Representatives of IFP are required to adhere and abide by the Privacy Policy and Requirements set by IFP. This includes the following:

a) The Privacy Policy released by IFP and available on the IFP website is to be adopted by all authorised representatives. No changes are to be made to this document unless special approval is sought.

b) All client information collected must be confirmed as true and correct by the client. This can be done in a variety of ways eg client signing Fact Find documents; Authority to Proceed/Implement; application forms; proposal forms; confirming in writing via email or post etc.

c) All client information must be retained in a secure manner. This includes ensuring only authorised persons are able to access client files in either hard copy or electronic versions. All electronic access should be limited by password protections and all hard copy documents must be retained in a lockable format when not in active use, with only authorised persons having access to the lockable format. Where there is a shared premise with another business that is not authorised through IFP, there must be very clear security measures in place for the retention of all client files – electronic or otherwise.

d) Physical transporting or sending of client information – when transporting or sending client information to other parties, you must first ensure that the other party is authorised to view such information ie the client has provided permission for the other party to access and view their information. If transporting or sending client information, a high level of security must be exercised.

    i. ***Electronic information:*** If sending or transporting client information electronically either through saving information on USB or other transportable drives or through means such as DropBox; SharePoint or other sharing applications, the files/folders must be password protected or there must be confirmation that only the persons sent the links can view the shared information.

    ii. ***Hard copy file transfers***: when transporting files in hard copy, the files must be secured in a manner to ensure that should they be dropped, documents will remain secure and not seen by others not authorised to view that documentation. Hard copy files should not be stored in vehicles at any time and when being transported between locations, must be in the presence of an authorised person at all times. This means that files should not be kept in cars overnight or for extended periods; if you are taking hard copy documents to client meetings away from your office, these must be secured (in a bag etc preferably lockable) and the authorised representative must be vigilant at all times to ensure that files are not accessed by persons who are not authorised.

5 Resources

- Definitions
- Data Breach Response Plan
- Authority to Collect, Use and Disclose TFN Form

Definitions

Consent means express consent or implied consent.

Eligible data breach arises when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information in circumstances where unauthorised access is likely to occur;
- a reasonable person would conclude that the unauthorised access, disclosure or loss would likely result in serious harm to any of the individuals to whom the information relates; and
- IFP has not been able to prevent the likely risk of serious harm with remedial action.

Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

Sensitive information means:

(a) information or an opinion about an individual's:

i. racial or ethnic origin; or
ii. political opinions; or
iii. membership of a political association; or
iv. religious beliefs or affiliations; or
v. philosophical beliefs; or
vi. membership of a professional or trade association; or
vii. membership of a trade union; or
viii. 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; or

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

Serious harm is not defined in the Privacy Act 1988. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm.

Data Breach Response Plan

1. PURPOSE

The purpose of this plan is to ensure that IFP identifies and reports eligible data breaches to the Commissioner and affected individuals in a timely manner.

2. RESOURCES REQUIRED

Notifiable Data Breach statement – Form on the Commissioner's website

https://forms.uat.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB

3. PROCEDURE

1. IFP will consider if there has been a data breach that is likely to cause serious harm. When determining whether the data breach is likely to cause serious harm, the following factors will be considered:

   (a) the kind or kinds of information;

   (b) the sensitivity of the information;

   (c) whether the information is protected by one or more security measures;

   (d) if the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome;

   (e) the persons, or the kinds of persons, who have obtained, or who could obtain, the information;

   (f) if a security technology or methodology:

   - was used in relation to the information, and;
   - was designed to make the information unintelligible or meaningless to persons who are not authorised to obtain the information;

   (g) the likelihood that the persons, or the kinds of persons, who:

   - have obtained, or who could obtain, the information, and;
   - have, or are likely to have, the intention of causing harm to any of the individuals to whom the information relates;
   - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;

   (h) the nature of the harm; and

   (i) any other relevant matters.

2. Take remedial action that is likely to reduce the harm to the affected individuals.
3. Where IFP suspects an eligible data breach, IFP will carry out reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach.
4. IFP will complete the assessment within 30 days of becoming suspicious of an eligible data breach.
5. IFP will consider whether a reasonable person would conclude that the remedial actions have resulted in the data breach not likely to cause a serious harm to the affected individuals. **If it is likely the data breach will not result in serious harm, please refer to step 8.**
6. Once IFP becomes aware of the eligible data breach, the Responsible Manager/s will prepare a statement on the eligible data breach as soon as practicable. The eligible data breach statement should set out:
   (a) the identity and contact details of IFP;
   (b) a description of the eligible data breach that IFP has reasonable grounds to believe has happened;
   (c) the kind(s) of information concerned; and
   (d) recommendations about the steps that individuals should take in response to the eligible data breach that IFP has reasonable grounds to believe has happened.

   A copy of the eligible data breach statement will be provided to the Commissioner via the Notifiable Data Breach statement – Form on the Commissioner's website as soon as practicable.
7. Responsible Manager/s will take reasonable steps to notify the contents of the eligible data breach statement to the:
   (a) individuals to whom the relevant information relates; and
   (b) individuals who are at risk from the eligible data breach.
8. IFP will review the data breach and take action to prevent future breaches.

Appendix A – Sample Authority to Collect, Use and Disclose TFN Form

Client Name:	**TFN:**

Integrity Financial Planners Pty Ltd can collect, use and disclose your Tax File Number ("**TFN**") for lawful purposes with your consent under the Taxation Administration Act 1953, Superannuation Industry (Supervision) Act 1993 and other taxation law, superannuation law and personal assistance law as defined in the Privacy (Tax File Number) Rule 2015.

You authorise your TFN(s) as provided to be collected and maintained by Integrity Financial Planners Pty Ltd for the purposes of forwarding the TFN to financial institutions as requested or as necessary. You understand that a failure to provide your TFN is not an offence, however, a failure to provide a TFN to a product provider or service provider may require the product/service provider to deduct tax from the financial products held by you at the highest marginal tax rate.

Signature: _____

Name: _____

Date: _____

Signature: _____

Name: _____

Date: _____