Privacy Standard

Version 2.0
February 2018

Description:

This Standard is designed to enable individuals and practices to understand their obligations under the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

Notifiable Data Breaches to be reported to affected individuals and the Office of the Australian Information Commissioner (OAIC)

To be read in conjunction with the Information Security Standard and Advice Process Standards

> ! This standard is not a summary of Privacy law. Practices should obtain legal advice if further information about obligations under the Privacy Act/breaches of the Privacy Act are required.
>
> ! The APPs are found in the Privacy Act 1988 (Cth).

Key Principles:

Open and transparent management of Personal Information.
Effective and compliant collection, use, disclose, retain and destruction of Personal Information.

> ! Personal Information is any piece of data that could potentially identify a specific individual.

Tools and References:

Privacy Act 1988 (Privacy Act)
Corporations Act 2001
Spam Act 2003
Australian Privacy Principles
Information Security Standard
Advice Process Standards
Office of the Australian Information Commissioner (OAIC)
Notifiable Data Breaches Scheme (NDB Scheme)
Identifying Eligible Data Breaches
Data Breach Notification Guide

Further assistance:

advicerisk@ioof.com.au
professionalstandards@ioof.com.au
T: 1300 722 923

Version control

Version	Released	Owner	Approved by	Summary of changes	Next review
1.0	February 2016	Professional Standards	Risk & Compliance Board Committee	New adviser standard	February 2017
2.0	February 2018	Professional Standards	Head of Professional Development	Reporting of Notifiable Breaches (NDB Scheme)	February 2019

Table of Contents

Introduction

The Privacy Act and Australian Privacy Principles (APPs) obligations aim to improve the safety and security of all personal and sensitive information collected, held and used. To comply with the law, reasonable steps need to be taken in order to protect a client's personal and sensitive information from:

- misuse, interference or loss; and
- unauthorised access, modification or disclosure.

In instances where personal information is lost, or subjected to unauthorised access or disclosure, an assessment must be made to ascertain whether serious harm is likely to occur to any affected individuals, in which case it must be reported under the **Notifiable Data Breaches (NDB) Scheme**

Each practice needs to determine how and to what extent the requirements of this standard are being met.

A self-assessment tool to assist in identification of any gaps has been provided (Appendix A). Please engage your licensee supervisor (SDM, PDM, PDC etc) for assistance if required.

Any identified failings or suspected failing is required to be reported to the Advice Risk Team within 24 hours.

📖 Please see the Incident Notification Standard for more details.

Australian Privacy Principles

A snapshot of the APPs are listed below. This standard also advises what tools and templates you have been provided with to assist in meeting your obligations of the Privacy Act. This standard provides requirements and guidance to meet each of the APPs.

APP 1 – Open and transparent management of personal information
APP 2 – Anonymity and pseudonymity (Non Applicable due to Corporations Law requirements)
APP 3 – Collection of solicited personal information
APP 4 – Dealing with unsolicited personal information
APP 5 – Notification of collection of personal information
APP 6 – Use or disclosure of personal information
APP 7 – Direct marketing
APP 8 – Cross border disclosure of personal information
APP 9 – Adoption, use or disclosure of government related identifiers
APP 10 – Quality of personal information
APP 11 – Security of personal information
APP 12 – Access to personal information
APP 13 – Correction of personal information

APP 1, 3, 5 and 6 – Collection, Notification, Use and Disclosure

Practices are required to establish processes and procedures to appropriately manage the collection, destruction, use and security of client's personal information.

This includes the requirement to not collect personal information unless the information is reasonably necessary for one or more of your functions or activities; and not collect sensitive information unless the individual consents to the collection and the information is reasonably necessary for one or more of your functions or activities.

The Best Interests Standard, Advice Process Standards and Fact Find template provide the tools and requirements regarding the collection of the necessary personal information (and sensitive information) that is required in order to provide recommendations and advice so that the adviser can meet his/her best interests duty.

The FSG (Part A) contains information under the section called 'Privacy Statement' to ensure compliance with the requirements within APP1, 3, 5 and 6. The law requires you to notify clients about what personal information you will collect and how you use or disclose it, (including if you pass it on to third parties).

> **!** Every practice website must also contain a copy of the licensee approved **Privacy Statement**, accessed via the **Privacy link**. Practice website Privacy Statements must contain a link that refers clients to the **IOOF Privacy Policy**.

The Privacy Statement within the FSG and the IOOF Privacy Policy provides clients information on:

- how personal information will be used and disclosed;
- the purpose for why you collect, use and disclose personal information,
- how your client may access personal information about themselves that you hold and seek the correction of such information,
- if personal information is likely to be disclosed to a recipient overseas and the countries in which such recipients are likely to be located.
- how an individual may raise concerns or complain about a breach of the Australian Privacy Principles;

File notes are required to capture the client receipt of the FSG and the conversations confirming that privacy obligations were discussed and disclosed. The file notes should include any questions in relation to privacy and also reflect your responses to the client's questions.

The Fact Find "Client Declarations and Consent page" of the document contains references to privacy, including a requirement for the client to acknowledge that they have received a copy of the FSG and read and understood the Privacy Statement.

The SoA/RoA "Declaration and Consent page" contains references that the client has received the FSG and read and understood the Privacy statement

Product Disclosure Statements (PDS's) contain references to Privacy obligations including client consent to collection, use, storage and disclosure of personal information.

Additionally each practice must make the IOOF Privacy Policy available to all clients upon request.

APP 4, 10, 13– Updating and Correction of Personal Information and collection of non-solicited personal information

Personal information collected must be accurate, up-to-date and complete. Practices must ensure that personal information collected, particularly within application forms, is necessary and relevant to the advice provided to the client.

All practices must have a process to correct or update a client's personal information when it becomes known that information held is not accurate, up to date, complete, relevant and/or misleading. Once aware, or provided with updated client information, this information is required to be reflected within the practice's client file records, financial planning software, customer information databases and any other client record keeping systems.

Clients may also request to change their details held by product providers, with which they hold a financial product recommended by the practice. All practices must also establish a process to provide updated information to the relevant entities if the client provides updated information ***AND*** requests the practice to notify the product provider of the correction. This process should include warning clients that product providers may require direct client contact or may require this information to be provided on a specific form signed by the client before they will enact changes.

Additionally, where additional personal information has been received, that is not reasonably necessary for the advice (e.g. client gives you copies of their medical records without you asking for it, however you are not providing insurance advice) this information must be given back to the client or removed from the client file and destroyed in a secure manner (security bin, shredder etc).

APP 7 - Direct Marketing

Direct marketing is the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services. This covers communicating with an individual through a variety of channels including telephone, SMS, mail, email and online advertising.

When marketing directly to existing or prospective clients, compliance with APP 7, which specifically regulates the use of personal information for direct marketing, is required. See below for a summary of the key direct marketing requirements:

- The use or disclosure of personal information for the purpose of direct marketing is prohibited unless an exception applies.
- If an organisation uses an individual's personal information for the purposes of direct marketing and the individual requests that the organisation not use its personal information for that purpose, the organisation must comply with that request within a reasonable period. The organisation must, on request, provide its source for the individual's personal information, unless it is impracticable or unreasonable to do so.

> 📖 Please read **Chapter 7: Australian Privacy Principle 7 – Direct Marketing** – for further guidance. This is available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-7-app-7-direct-marketing

Anti-Hawking provisions

The Corporations Act prohibits selling of a financial product (including inviting an application), if the offer is made during or because of an unsolicited meeting or telephone call with a client or potential client, subject to certain exceptions.

ASIC considers that a meeting or phone call is 'unsolicited' unless it takes place in response to a positive, clear and informed request from a client or prospective client. Furthermore, solicitation requires a client to reasonably expect to discuss the specific products or classes of product in the meeting or telephone call. Therefore, if a client phones to discuss their personal insurance and is offered a managed investment product, this may be considered be unsolicited in relation to the managed investment product offer as this is not something the client wanted to discuss.

When making unsolicited telephone calls, we expect that you:

1) Only contact clients during the hours prescribed by the regulations and only if the person is not listed on your practice's "No Contact/No Call" Register; and
2) Give the client an opportunity to:
    - Register on your practices "No Contact/No Call" Register at no cost to the client; and
    - Select the time and frequency of any future contacts.

Do not make unsolicited telephone calls concerning securities.

Additionally all practices should work closely with business partners to ensure compliance when sharing client information for marketing purposes.

SPAM Act

The Spam Act 2003 ('Act') regulates the use of commercial electronic messages (CEMs). CEMs include any email, instant messaging, SMS and other mobile phone messaging that contains an element of offering or advertising of goods or services; including a financial service.

> **!** Attachments to an email are considered to be part of that email for spam purposes.

To comply with the legislation:

- Unsolicited CEMs must not be sent. A CEM is unsolicited if it occurs without the recipients prior consent (expressed or reasonably inferred).
- CEMs must include information about the individual or organisation that authorised the sending of the message.
- CEMs must contain a functional unsubscribe facility (Opt out).
- Address-harvesting software must not be supplied, acquired or used. Address-harvesting software is defined as software that is specifically designed or marketed for use for searching the internet for electronic addresses and collecting, compiling, capturing or otherwise harvesting those electronic addresses.

> **!** Spam excludes electronic messages that do not contain an element of offering or advertising of goods or services, which is factual information only. This includes answering a specific query with no added marketing and service messages

Managing the Opt-out process

All practices are required to develop a process to manage clients requesting to opt-out of direct marketing activity.

This may include reviewing the client database to group the types of marketing material clients have chosen to opt out of e.g. all marketing material or material in respect of a particular service you provide.

> **!** It's important to make clients aware that material such as newsletters, are part of their contractual arrangements (e.g. service package). Additionally there are documents required by law that will be to send them such as your Fee Disclosure Statement (FDS). The customer cannot opt out of receiving these documents.

Opt out wording should be incorporated on all direct marketing activity. See below for a suggested appropriate disclaimer:

From time to time we may send you informative updates and details of the range of services we can provide. If you no longer want to receive any of this information please [insert method] to opt out. Note: If, as part of our contractual arrangements, you have agreed to receive certain material from us (e.g. our newsletter) please contact the office if you need to alter this arrangement.

Managing Prospective clients

When holding lists of prospective clients to whom marketing material has been sent but no financial service provided all hardcopy and electronic versions of their personal information should be destroyed when that information is of no further use. As a guide-line we suggest within 12 months of distributing the marketing piece.

> **!** Any list of prospective clients must be accompanied with where that list has been sourced.

APP 8 - Off Shoring arrangements

APP 8 requires that you undertake reasonable investigations to ensure that an overseas recipient of the personal information of your clients does not breach the APPs in respect to that information.

To assist a self-assessment tool has been developed (Please see Appendix B). The tool records where a client's personal information is being given to third party business service provider. For all new arrangements and existing businesses this should be completed by following the steps below:

Step 1: Any client referred to an Australian on-shore third party for professional services including legal, accounting, general insurance, stockbroking, mortgages etc. should be recorded in the self-assessment tool. If this outfit has any off-shore (overseas) element that you are aware of this should be noted. If the outfit sends personal information overseas, the on-shore outfit must take reasonable steps to ensure the overseas recipient complies with the APPs in respect of that personal information

Step 2: Off-shore third party outfits which support your practice operations in any way (for example overseas based administration or paraplanning service) should be recorded on the spreadsheet. The country from which the entity operates should also be included.

> **!** If personal information via referral/business service/partnership will be disclosed to recipients located in countries which are not listed in the IOOF Privacy Policy, the countries must be listed in Part B of your FSG.

Step 3: Make reasonable enquiries with the on and off-shore referral/business partners to ensure you are able to comply with APP 8. Reasonable enquiries require:

- A letter/email template to send to on-shore referral and business partners to enquire if they send any client information off-shore, and if so, asking for more information on these arrangements. The letter/email also requests that they confirm to you in writing that they will adhere to the APPs.
- A letter/email template to send to any off-shore business partners who use client information, requesting they confirm with you in writing that they understand and will adhere to the APPs.

Please see an email/letter template to use for the above communication in Appendix C

Step 4: Retain the written confirmation with the self-assessment tool (Appendix B)

Step 5: Continue to implement the above process for all new referrer/business service provider agreements/arrangements.

In addition to the letter confirmation, such an acknowledgement should be contained in any agreement with the referrer/business service provider.

Please contact Practice Manager/State Development Manager for guidance with respect to any referrer/service providers who off-shore client information but refuse to comply with the APPs.

APP 9 – Adoption, Use or Disclosure of Government Identifiers

Unless required or authorised by an Australian law or a court/tribunal order, practices must not:

- adopt a government related identifier (eg. tax file numbers) of an individual to use as an identifier of the individual; or
- use or disclose a government related identifier of an individual

Tax file numbers (TFN)

The TFN Guidelines instruct how TFN information should be collected, stored, used, disclosed and kept safe.

TFN guidelines only allow TFNs from individuals and other TFN recipients be requested or collected only for a purpose authorised by taxation law, personal assistance law or superannuation law.

When requesting an individual's TFN, reasonable steps must be taken to:

Ensure that individuals are informed of: • taxation law, personal assistance law or superannuation law which authorises you to request or collect the TFN; • the purpose(s) for which the TFN is requested or collected; • declining to quote a TFN is not an offence; and • the consequences of declining to quote a TFN
Ensure that the manner of collection does not unreasonably intrude on the individual's affairs
Only request or collect information that is necessary and relevant to the purpose of collection under applicable taxation law, personal assistance law or superannuation law
Protect clients' tax file numbers from misuse and loss
Ensure that access to records containing TFNs is restricted to those individuals who need to handle the information for the purpose for which it was given
Securely destroy or permanently de-identify TFNs where they are no longer: • required by law to be retained, or • necessary for a purpose under taxation law, personal assistance law or superannuation law (including the administration of such law)

APP 11 – Security of Personal Information

Where information is no longer required for the purpose for which it was collected and the practice is not required by law to retain it, the Privacy Act requires (under APP 11) that it be destroyed or de-identified. The Corporations Act 2001 (Cth) and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) provide minimum requirements with respect to retention of information. You are obligated to read the Information Security Standard.

Summary of the Information Security Standard

The Information Security standard provides the requirements and guidance that all practices, , advisers, staff/employees and contractors are required to abide by to meet APP 11 and your licensee's Information Security requirements. The standard provides requirements that practices and advisers must follow for:

- Personal Information Security & Destruction
- Information Management requirements
- Personal and Practice email/webmail
- Password protection
- Information and Data Security
- Practice Protocols
- Physical security
- Sending information electronically

APP 12 – Access to Personal Information

Requests for access to personal information by an individual must be provided to that individual. It is prohibited to provide spouse/partner information, unless the individual requesting access to personal information has provided a copy of a Power of Attorney (PoA) which authorises that individual with the legal ability to request information.

> ✓ A number of parties may request access to file and file notes. Ensure that the information captured is professional at all times. Do not make notes/comments that could be regarded as derogatory/offensive to that individual.

There may be incidents where information would **not** be able to be given to the individual, for example:-

- where there is an ongoing complaint/investigation with respect to the individual or their client file.
- giving access would pose a serious threat to the life, health or safety of the individual,
- giving access would have an unreasonable impact on the privacy of other individuals,
- the information relates to existing or anticipated legal proceedings, and would not be accessible by the process of discovery in those proceedings,
- giving access would be unlawful.

Notifiable Data Breaches Scheme (NDB Scheme)

From 22 February 2018, an amendment to the Privacy Act 1988 introduces mandatory data breach notification requirements, applicable to all **eligible data breaches**.

Under this legislation, there is a legal requirement that any **affected individuals**, as well as the **Office of the Australian Information Commissioner (OAIC)**, be notified in instances where a data breach is **likely to result in serious harm** to any affected individuals.

The **likely risk of serious harm** could include physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of harm that a **reasonable person** would identify as a possible outcome of the data breach, eg:

- identity theft
- significant financial loss
- threats to physical safety
- loss of business or employment opportunities
- workplace or social bullying or marginalisation

Why the need to notify?

The **NDB Scheme** was was introduced to:

- strengthen the protections afforded to everyone's personal information
- improve transparency in the way that organisations respond to serious data breaches
- give individuals the opportunity to take steps to minimise the damage that can result from unauthorised use of their personal information

What is a Data Breach?

A data breach occurs when **personal information** about one or more individuals (the **affected individuals**) held by an organisation is lost, or subjected to unauthorised access or disclosure.

Examples of a data breach include when (see appendix D for further examples of NDBs):

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person
- paper records stolen from insecure recycling or rubbish bins
- an individual deceiving an organisation into improperly releasing the personal information of another person

Types of Personal Information that are more likely to cause an individual serious harm if compromised include:

- sensitive information such as information about an individual's health,
- documents commonly used for identity fraud such as driver licence or Medicare card details
- financial information
- a combination of personal information

Under the **NDB Scheme**, when it becomes evident that a **data breach** has occurred, the breach must immediately be assessed to establish whether or not it is a **Notifiable Data Breach**, and if so necessary actions taken as soon as practicable to ensure that any affected individuals and the OAIC are notified accordingly.

ACTIONS TO TAKE IN THE EVENT OF A DATA BREACH

Data Breach Response Guidance is in place at licensee level to ensure that in the event of a data breach the following actions are taken:

- containment and assessment
- evaluation of associated risks to affected individuals
- notification of affected individuals and OAIC
- prevention of future breaches

From an **adviser/practice** perspective, in the event of any data breach being identified, **immediate** steps should be taken to:

- contain the data breach, assess and document that no further clients are affected, and that the potential for further harm has been limited
- take immediate remediation steps where possible
- engage your **licensee supervisor** and **immediately** inform the **Advice Risk** team (advicerisk@ioof.com.au). Consult with them to evaluate the breach using the **Notifiable Data Breach Assessment Guide,** to establish whether or not it meets the criteria for notifying the OAIC
- If required, **Advice Risk** will escalate to the relevant forum so that the OAIC and affected individuals are notified.

> **!** Not all data breaches are eligible for notification. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the OAIC.

Practice Training Requirements

All practices are required to train staff (permanent or temporary) and contractors who have access to client information about their privacy obligations. The following is a recommended Privacy induction process:

1. Review the Privacy Standard, Information Security Standard and the Practice Privacy Declaration and
2. Discuss privacy obligations comprehensively including what changes could be implemented to improve privacy and who will implement the changes.
3. Discuss the Information Security Standard obligations comprehensively.
4. Ensure that all existing employees/contractors and all new employees/contractors sign the Practice Privacy Declaration and retain this within the employee's file or the practice's privacy file.

> **!** Creating a Practice Privacy file is required to confirm a practice understands and has agreed to comply with their privacy obligations.

All advisers, practice staff and contractors who have access to client information are required to declare that they will adhere to the APPs. To assist in understanding Privacy obligations an Internal Practice Training Declaration, which outlines privacy requirements, has been created (Appendix E).

Appendix A - Privacy Checklist

Considerations below should be reviewed and evaluated in the context of your practice and may need to be scaled up or down according to the size and complexity of your business.

Area	Practice Confirmation – The following processes/procedures/requirements have been implemented within the practice to meet the Privacy Standard Requirements
APP 1 – Open and transparent management of personal information	
APP 3 – Collection of solicited personal information	
APP 4 – Dealing with unsolicited personal information	
APP 5 – Notification of collection	
APP 6 – Use or disclosure	
APP 7 – Direct marketing	
APP 8 – Cross border disclosure	
APP 9 – Adoption, use or disclosure of government related identifiers	
APP 10 – Quality	
APP 11 – Security	
APP 12 – Access	
Notifiable Data Breach (NDB) Scheme – ACTIONS TO TAKE IN THE EVENT OF A DATA BREACH	
APP 13 – Correction	
Practice Training	Confirmed that the practice has this requirement included within their induction of new employees/contractors. This information is saved in_____

Appendix B – APP 8 – Relationship Self-Assessment

Practice name, Owner of Privacy Self -Assessment in Practice, Contact phone number						
List the name of **all** third parties (excluding clients and their lawyers and accountants) but including referral sources. ***Referral sources is limited to entities your practice refers clients to NOT those who refer prospects to you***. Also capture other third party outfits supporting operations such as administration, paraplanning and IT.						
Name of third party entity	**Key Contact and Address**	**Is this entity based overseas?**	**If NO, does the entity send personal information offshore (either to a third party or an offshore subsidiary)?**	**If you have answered YES to either or both questions, please detail services being provided**	**Will the services referred to in column involve the provision of a client's personal information (As defined in the APPs) to that entity?**	**Name of country if offshore services are provided/held**
		YES/NO	**YES/NO**			
Important notes:						
Identify all relationships (on and off-shore) as you will send letters to all key third party relationships.						
Where you disclose personal information to recipients located in countries which are not listed in the Privacy Policy the clients must be informed of those countries in the Adviser Profile of the FSG.						

Appendix C – Letter to ON-SHORE Referral and Business Partner

WORDING TO SEND TO ON-SHORE REFERRAL AND BUSINESS PARTNERS:

Dear <referral/business partner name>

Requirements under the Privacy Act

<As a valued business partner we may refer clients to you who can benefit from your expertise and services from time to time.>

OR

<As a valued business partner we engage you to support us to deliver our business operations.>

Following changes to the Privacy Act (which took effect on 12 March 2014), the Australian Privacy Principles (APPs) have replaced the National Privacy Principals (NPPs) and all Australian businesses have increased obligations to manage and protect client information.

Under the new APP8 we must take reasonable steps to ensure any overseas recipient of our customers' personal information complies with the APPs. If you are off-shoring or any of your onshore suppliers are offshoring any part of business operations (e.g. to Singapore, Malaysia, India etc.) and need to send personal client information off-shore please call or email me with:

- the type of client information you send off-shore
- information on the type of service the off-shore provider supplies to you
- the country the information is sent to
- the steps that you have taken to ensure that the off-shore provider has agreed to comply with the APPs *i.e. a provision in your agreement with the entity or that they have formally written to you stating they will comply.*

If you do not send any personal client information off-shore then there is no need to respond to this mail.

I look forward to our continued professional business partnership.

Yours sincerely,

<Insert your sign-off signature>

Appendix D – Identifying Notifiable Data Breaches

The notifiable data breaches (NDB) scheme requires regulated entities to notify particular individuals and the OAIC about 'eligible data breaches'. A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

Whether a data breach is likely to result in serious harm requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

Not all data breaches are eligible. For example, if an entity acts quickly to remediate a data breach, and as a result of this action the data breach is not likely to result in serious harm, there is no requirement to notify any individuals or the OAIC (see Example 1).

An eligible data breach arises when the following three criteria are satisfied (see Example 2):

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
2. this is likely to result in serious harm to one or more individuals, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

Example 1 — email sent to the wrong recipient contained before serious harm can occur

An adviser accidentally sends an email with an encrypted attachment to the wrong client. The attachment contains a Statement of Advice and other personal information. The adviser realises the error, and contacts recipient to delete the email with the attachment. The recipient confirms they have not accessed the file, and that they have deleted the email.

The adviser contacts their licensee supervisor and together they assess the remedial action taken, to conclude that whilst the file included personal information about the individual's name, address, date of birth, business structure and ABN, personal finances and superannuation policy numbers, the assurance that the incorrect recipient (another client) deleted the file has prevented the likely risk of serious harm to the client, particularly as the attachment was encrypted (NB: encryption passwords should never be sent in the same email as the encrypted document). As a consequence, the adviser and supervisor determine that it is not an eligible data breach, and no further action is required.

Example 2 — loss of unencrypted storage media containing personal information

An unencrypted memory stick containing the current files of 3 clients on which an adviser is planning to work on from home over the weekend goes missing between leaving the office on Friday afternoon and getting home. Once the Adviser becomes aware that the memory stick is lost, he conducts an extensive search but fails to locate it. The information contained in the client files includes the names, salary information, TFNs, home addresses, phone numbers, birth dates, and in some cases health information (including disability information) of the clients. As the data on the memory stick is not encrypted, and there is a chance that the memory stick was lost outside of the Adviser Practice's premises, the Adviser concludes that unauthorised disclosure may likely occur.

Due to the sensitivity of the unencrypted information – not only the extent and variety of the information, but also the inclusion of financial and health information in the files – the

Adviser's risk assessment finds that there is a likely risk of serious harm to at least one of the individuals whose personal information is involved in the data breach. On this basis, the **Adviser immediately engages their licensee supervisor (SDM, PDM, PDC etc) and Advice Risk to assess whether or not it may be an eligible data breach for the purposes of the NDB scheme.** The Adviser also takes immediate steps to contain and remediate the breach by contacting each of the three clients to explain the loss of the memory device and what types of personal information were involved, as well as recommending mitigating steps that can be taken to limit and/or eliminate any risk of harm to themselves. If determined that a Notifiable Data Breach has occurred, the Advice Risk team will assist in preparing a statement to notify the OAIC, and affected individuals.

Appendix E – Internal Practice Training Declaration

[on letterhead of practice]

Internal Practice Training Declaration Protecting our client's privacy

Every person who is:

- an employee of this practice; or
- a contractor to this practice,

and has access to client information, is required to take reasonable steps to meet the requirements of the Privacy Act.

We pride ourselves on applying a high standard of professionalism when dealing with our clients who entrust us with personal information in relation to their finances and other matters such as details of their business, family and health.

As a valued team member you understand that our clients consent to us collecting their information and disclosing it only for the purpose of providing them with financial products and services.

Your obligations

At all times you will take reasonable steps to keep our clients' personal information protected from:

1. misuse, interference or loss; and
2. unauthorised access, modification or disclosure.

At a minimum, you agree:

- to read and comply with the Privacy Statement set out in our Financial Services Guide;
- to read and comply with the Privacy Standard
- to read and comply with the Information Security Standard
- not to leave client files open;
- not to leave client information where other staff can view that information;
- to ensure that Tax File Numbers and other Government identifiers are not used to identify a client on our systems;
- to delete Tax File Numbers and other Government identifiers from the client file or system(s) when there is no further reason to hold this information;
- to implement identification procedures, such as:

  - ensuring that you only provide information that is in relation to the individual client and not in relation to their spouse/partner etc (unless you have the relevant power of attorney documents on file)
  - ensuring that we hold an authority to release the information where the person requesting the information is not the client whose information is being requested;
- to observe "Do Not Contact" notices unless informed to do otherwise by your [practice manager - insert appropriate title] for the purpose of complying with a separate legal obligation;
- to familiarise yourself with the full IOOF Privacy Policy; and
- not to discuss or disclose any of our clients' information with any person other than in accordance with the Privacy Statement.

Declaration

I **declare** that I have read and understood the matters referred to in this document and the Privacy Statement and agree to take the steps outlined above:

_____

Signature

_____

Full name (PRINT)

_____

Position

_____

Date