

CLIENT FILE MANAGEMENT POLICY

Version: 1.02

Last Updated 08.01.18

THE AIM OF THIS POLICY

The policy sets out the requirements for ensuring effective client record management and file maintenance.

WHO THIS POLICY APPLIES TO

This policy applies to all staff of Insight Investment Partners.

WHAT THIS POLICY COVERS

This policy covers:

- What You Must Do
 - General Obligations
 - Tax File Numbers
 - Electronic Storage
 - File Notes
- What You Must Not Do
 - General Obligations
 - Tax File Numbers
- Good Operating Practice
 - Electronic Storage
- FAQ

What You Must Do

GENERAL OBLIGATIONS

- Establish and maintain a file whenever you provide any form of advice and/or services to any client or potential clients (i.e. where an interview or discussion has taken place but business has not been written).
- Maintain up-to-date and accurate file information, encompassing all aspects of the advice and/or services provided. This includes evidence of all advice documentation and supporting documentation, provided or received and comprehensive file notes for every discussion and interaction, in relation to your client.
- Ensure that you adhere to the privacy requirements within the Data Collection Policy when collecting, storing, disclosing and using a client's information.
- Take reasonable steps to protect a client's personal information from:
 - misuse;
 - interference;
 - loss;
 - unauthorised access/disclosure;
 - modification.
- Ensure that all files including temporary files are stored securely.
- Separate all financial planning client files from any other file you have for the client (e.g. accounting file); refer to the Separation of Business Adviser Guide within the Identification and Promotional Material Policy.

- Ensure that your records support all communication and decision-making and enable you and Insight Investment Partners to:
 - demonstrate that you have acted in your client best interests;
 - provide a record of conversations between you and the client;
 - provide evidence of any advice/services provided and that the appropriate advice has been given to your client;
 - rely on documentary evidence when handling a client complaint (and in some cases providing evidence in matters referred to the courts or relating to a regulatory enquiry);
 - provide evidence of business transactions;
 - ensure that relationships with your clients are not adversely impacted as a result of having to reconstruct lost or misplaced files in order to service these clients efficiently and effectively;
 - meet your legal and statutory requirements and stakeholder obligations.
- Ensure documents include client signatures to evidence their receipt and acceptance by the client. This excludes online product application processes where the product provider uses an alternative method to verify client receipt/acceptance.
- Provide copies of client files upon request by the Responsible Manager.
- Obtain client consent prior to and at the beginning of a recorded conversation (required each time). This includes verbal consent from and identifying all participants on the recording.
- Maintain client files for seven (7) years from when they cease to be a client.
- Maintain a list of archived files, detailing:
 - name of client;
 - name of adviser;
 - practice or office name;
 - date of last contact; and
 - professional archivist (e.g. Pickford's) record number.

TAX FILE NUMBERS

- Ensure clients complete the TFN Consent Form prior to collecting their TFN (available in the Fact Find).
- Only use a client's TFN for the purpose for which it was collected as specified in the TFN Consent Form.
- Remove a client's TFN from their file in the circumstances listed below. This includes removal from all documents and from your Client Relationship Management (CRM) software e.g. XPLAN), such that the TFN is illegible. Supporting file notes must be maintained.
 - They do not wish to receive ongoing advice.
 - They cancel their Ongoing Advice Service Agreement (OASA).
 - They withdraw their consent for their TFN to be retained.

ELECTRONIC STORAGE

- Maintain the same standard of security for electronic files as paper based records to ensure client confidentiality and meet privacy standards.
- Be able to demonstrate the reliability, integrity, and accessibility of scanned documents, such that the Responsible Manager can show the copy is a true duplicate of the original and has not been altered or tampered with.
- Back up records regularly (daily recommended) and stored offsite (weekly recommended).
- Conduct regular testing to ensure records continue to be retrievable and readable.

- Upload the final version of an advice document as presented to the client. Draft versions are not acceptable. The Authority to Proceed may be uploaded separately when signed.
- Ensure documents are protected (e.g. using a PDF format) such that they cannot be altered in any way and remain true copies of the original records.
- Ensure that a scanned document is of the same quality as the original when reproduced.
- Ensure that the software:
 - automatically records and dates documents as they are added with no ability to backdate/alter records; and
 - is protected from unauthorised access including password protection.

FILE NOTES

- Maintain file notes for all contact you have with the client and any party that is relevant to your relationship with the client and the financial services you provide to the client, for example (not exhaustive):
 - the client's other professional services (e.g. accountant, solicitor);
 - product providers;
 - internal administration area or any external body (e.g. ASIC, ATO, Centrelink).
- Ensure your file notes are:
 - a true and correct reflection of events;
 - written in English, be legible and make sense to any third party such as an auditor or regulatory body, and;
 - made as soon as possible after the event.

What You Must Not Do

GENERAL OBLIGATIONS

- Maintain records of client conversations on your laptop/tablet; they must be uploaded to your secure electronic storage.
- Maintain client credit card details on file. This information must be scored out such that it is illegible once the corresponding advice has been implemented. Given the difficulty in redacting information from audio recordings, credit card details must not be recorded during a conversation.
- Dispose of client files with normal office waste; a secure bin must be used.
- Destroy hard copies of documents/files:
 - that are required to be returned to the client;
 - represent a limited power of attorney granted to the adviser for the purpose of providing an MDA service;
 - that are retained in hard copy on behalf of a product provider where an online application has been submitted (only if indicated by the provider);
 - in any circumstance where the licensee has directed the retention of a hard copy file.

TAX FILE NUMBERS

- Divulge a client's TFN to a third party, other than as authorised by the client.
- Use this information where it is disclosed incidentally e.g. as part of an income tax return or PAYG summary.
- Record this information in an audio recording with your clients.
- Use a client's TFN as a form of identification to gather information or as a client identifier.

FAQ

Questions	Answers
Do I need to create and maintain hard copy client files?	With the exception of certain documents as set out in this policy (You Must Not > General Obligations), you are not required to create and maintain hard copy client files.
What documents must be kept on a client file?	All copies of signed documents, information collected from or given to the client, comprehensive file notes of all meetings and telephone discussions, all relevant disclosure documents including the versions and dates provided, as well as all other relevant correspondence with the client, or a third party, or licensee in relation to the client.
If a client requests information from their file, what information can I provide to them?	Contact the Compliance Manager, who will manage any requests received from a client to access their client file.