Privacy Policy

November 2023

Kestrel Capital Pty Limited
ABN 68 061 515 062 AFSL 227065

Suite 301, 55 Lime Street
Sydney NSW 2000

Title of document	Privacy Policy
Description	This policy provides guidance to assist with complying with the *Privacy Act 1988* (Cth) ("**Privacy Act**") and the Australian Privacy Principles in protecting the personal information the Company holds about its clients.
Scope	All officers and employees of Kestrel Capital and its subsidiaries
Policy Owner	Compliance Officer or Board delegate
Policy Approver	Kestrel Capital Board
Effective Date	November 2023
Review Date	November 2026 or on material change
Related documents	• Breach Reporting Policy

Table of Contents

1. Definitions....4
2. Introduction....5
3. When Does This Policy Apply?....5
4. Privacy Statement....5
5. Personal Information (Other Than Sensitive Information)....6
6. Sensitive Information....6
7. Means of Collection....7
8. Information Collected by the Company....7
9. Purpose of Collection....7
10. Dealing With Unsolicited Personal Information....8
11. Notification of Collection....8
12. Use or Disclosure....9
13. Direct Marketing....10
14. Exception - Personal Information Other Than Sensitive Information....10
15. Exception - Sensitive Information....10
16. Requests to Stop Direct Marketing....11
17. Disclosing Personal Information to Cross Border Recipients....11
18. Adoption of Government Related Identifiers....12
19. Use or Disclosure of Government Related Identifiers....12
20. Quality of Personal Information....12
21. Security of Personal Information....12
22. Storage of Personal Information....13
23. Access....13
24. Exceptions....13
25. Refusal to Give Access....14
26. Correction of Information....14
27. Refusal to Correct Information....14
28. Request from a Client to Associate A Statement with Their Information....15
29. Dealing with Requests....15
30. Complaints....15
31. Notifiable Data Breaches Scheme....16
32. Policy Breaches....16
33. Retention of Notifiable Data Breach Forms....16
34. Policy Review....17

1. Definitions

APP entity means an agency or organisation as defined in section 6 of the Privacy Act

Australian law means:

(a) an Act of the Commonwealth or of a State or Territory; or

(b) regulations, or any other instrument, made under such an Act; or

(c) a Norfolk Island enactment; or

(d) a rule of common law or equity.

Collects means Kestrel Capital collects personal information only if the Company collects the personal information for inclusion in a record or generally available publication

Court/tribunal order means an order, direction or other instrument made by:

(a) a court; or

(b) a tribunal; or

(c) a judge (including a judge acting in a personal capacity) or a person acting as a judge; or

(d) a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or

(e) a member or an officer of a tribunal;

and includes an order, direction or other instrument that is of an interim or interlocutory nature.

De-identified means personal information is *de-identified* if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

Eligible Data Breach occurs:

(a) where there has been unauthorised access of unauthorised disclosure of personal information, or a loss of personal information, that the Company holds; and

(b) the unauthorised access or unauthorised disclosure is likely to result in serious harm to one or more clients; and

(c) Kestrel Capital is not able to prevent the likely risk of serious harm with remedial action.

Holds means where the Company has possession or control of a record that contains the personal information.

Identifier of an individual means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include:

(a) the individual's name; or

(b) the individual's ABN (within the meaning of the A New Tax System (Australian Business Number) Act 1999); or

(c) anything else prescribed by the regulations.

Kestrel Capital, KC or the Company means Kestrel Capital Pty Limited ACN 061 515 062

Permitted general situation as defined in s16A of the Privacy Act

Permitted health situation as defined in s16B of the Privacy Act

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

(a) whether the information or opinion is true or not; and

(b) 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) sexual orientation or practices; or

(ix) 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.

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

(e) biometric templates.

2. Introduction

2.1. As part of the Company's process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, Company has adopted this Privacy Policy ("**Policy**") to manage personal information in an open and transparent manner.

2.2. The provisions of this Policy will assist the Company in complying with the requirements of the *Privacy Act 1988* (Cth) ("**Privacy Act**") and the Australian Privacy Principles in protecting the personal information the Company holds about its clients.

3. When Does This Policy Apply?

3.1. This Policy applies to all representatives and employees of the Company at all times and the requirements remain in force on an ongoing basis.

4. Privacy Statement

4.1. The Company's board must ensure that at all times the provisions of this policy are implemented in the day to day running of the Company.

4.2. The board or its delegate must ensure that at all times this Policy:

4.2.1. is current and reflects the latest applicable Australian laws; and

4.2.2. contains the following information:

(a) the kinds of personal information that the Company collects and holds;

(b) how the Company collects and holds personal information;

(c) the purposes for which the Company collects, holds, uses and discloses personal information;

(d) how an individual may complain about a breach of the Australian Privacy Principles, or other relevant legislation that binds the Company, and how the Company will deal with such a complaint;

(e) whether the Company is likely to disclose personal information to overseas recipients;

(f) if the Company is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in this policy

4.3. The Company must ensure that the Company's Privacy Statement is available free of charge and in such form as appropriate. The Company will make the Privacy Statement available on its website.

4.4. If the Privacy Statement is requested in a particular form, the Company will take such steps as are reasonable to provide the Privacy Statement in the form requested. We collect personal information when it is reasonably necessary for one or more of our functions or activities.

5. Personal Information (Other Than Sensitive Information)

5.1. The Company must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the Company's functions or activities.

5.2. The Company's functions or activities include:

(a) providing customers with the products and services they request and, unless they tell us otherwise, to provide information on products and services offered by us and external product and service providers for whom we act as agent. (If you have provided us with your email or mobile phone details, we may provide information to you electronically with respect to those products and services);

(b) complying with our legal obligations;

(c) monitoring and evaluating products and services;

(d) gathering and aggregating information for statistical, prudential, actuarial and research purpose;

(e) assisting customers with queries; and

(f) taking measures to detect and prevent frauds.

6. Sensitive Information

6.1. The Company must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and the information is reasonably necessary for one or more of the Company's functions or activities (as described in section 5.2); or

(b) the collection of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(c) a permitted general situation exists in relation to the collection of the information by the Company; or

(d) a permitted health situation exists in relation to the collection of the information by the Company.

7. Means of Collection

7.1. The Company must only collect personal information by lawful and fair means.

7.2. The Company must only collect personal information about an individual from the individual (rather than someone else), unless it is unreasonable or impracticable to do so or the individual has instructed the Company to liaise with someone else.

7.3. The Company will collect personal information from an individual when:

(a) The Company's Application Form is completed;

(b) a Client provides the information to the Company's representatives over the telephone or via email; or

(c) a Client provides the information to the Company on the website.

8. Information Collected by the Company

8.1. The information the Company collects may include the following:

(a) name;

(b) date of birth;

(c) postal or email address; or

(d) phone numbers;

(e) other information the Company considers necessary to their functions and activities.

9. Purpose of Collection

9.1. If an individual or an entity in which they hold a beneficial interest is acquiring or has acquired a product or service from the Company, the individual's personal information will be collected and held for the purposes of:

(a) checking whether an individual is eligible for the Company's product or service;

(b) providing the individual with the Company's product or service;

(c) managing and administering the Company's product or service;

(d) protecting against fraud, crime or other activity which may cause harm in relation to the Company's products or services;

(e) complying with legislative and regulatory requirements in any jurisdiction; and

(f) to assist the Company in the running of its business.

9.2. The Company may also collect personal information for the purposes of letting an individual know about products or services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section 13 for further information - Direct marketing exceptions requests to stop.

10. Dealing With Unsolicited Personal Information

10.1. If the Company:

(a) receives personal information about an individual; and

(b) the information is not solicited by the Company.

The Company must, within a reasonable period after receiving the information, determine whether or not it was permitted to collect the information under section 9 above.

10.2. The Company may use or disclose the personal information for the purposes of making the determination under paragraph 10.1.

10.3. If the Company:

(a) determines that it could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record,

the Company must as soon as practicable, destroy the information or ensure that the information is de-identified, only if it is lawful and reasonable to do so.

11. Notification of Collection

11.1. This section 11 applies to:

(c) solicited information; and

(d) unsolicited information to which section 10 does not apply.

11.2. The Company must notify the individual of the following matters in the Privacy Statement:

(a) the Company's identity and contact details;

(b) if the Company collects the personal information from a third party or the individual is not aware that the Company has collected the personal information, the fact that the Company so collects, or has collected the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a Court/Tribunal order, the fact that the collection is so required or authorised (including the details of the law or court);

(d) the purposes for which the Company collects the personal information;

(e) the main consequences (if any) for the individual if the information is not collected by the Company;

(f) any other entities to which the Company usually discloses personal information of the kind collected by the Company;

(g) that the Company's Privacy Statement and this Privacy Policy contains information about how the individual may access the personal information about the individual that is held by the Company and seek correction of such information;

(h) that the Company's Privacy Statement contains information about how the individual may complain about a breach of the Australian Privacy Principles and how the Company will deal with such a complaint;

(i) whether the Company will disclose the personal information to overseas recipients; and

(j) if the Company discloses the personal information to overseas recipients – the countries in which such recipients will be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

12. Use or Disclosure

12.1. Where the Company holds personal information about an individual that was collected for a particular purpose ("**the primary purpose**"), the Company must not use or disclose the information for another purpose ("**the secondary purpose**") unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) the individual would reasonably expect the Company to use or disclose the information for the secondary purpose and the secondary purpose is:

(c) directly related to the primary purpose (if the information is sensitive information); or

(d) related to the primary purpose (if the information is not sensitive information);

(e) the use or disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(f) a permitted general situation exists in relation to the use or disclosure of the information by the Company; or

(g) the Company reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

12.2. Where the Company uses or discloses personal information in accordance with section 12.1(e)(g), the Company will keep a copy of this disclosure (e.g.: the email or letter used to do so).

12.3. This section 12 does not apply to:

(a) personal information for the purposes of direct marketing; or

(b) government related identifiers.

12.4. If the Company collects personal information from a related body corporate, this section 12 applies as if the Company's primary purpose for the collection was the primary purpose for which the related body corporate collected the information

12.5. Insert defined company name] may disclose personal information collected from clients and prospective clients to the following:

(a) organisations involved in providing, managing or administering the Company's product or service such as third-party suppliers, e.g. printers, posting services, and our advisers;

(b) organisations involved in maintaining, reviewing and developing the Company's business systems, procedures and infrastructure, including testing or upgrading the Company's computer systems;

(c) organisations involved in a corporate re-organisation;

(d) organisations involved in the payments system, including financial institutions, merchants and payment organisations;

(e) organisations involved in product planning and development;

(f) other organisations, who jointly with the Company's, provide its products or services;

(g) authorised representatives who provide the Company's products or services on its behalf;

(h) the individual's representatives, including your legal advisers;

(i) debt collectors;

(j) the Company's financial advisers, legal advisers or auditors;

(k) fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;

(l) external dispute resolution schemes;

(m) regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

13. Direct Marketing

13.1. The Company must not use or disclose the personal information it holds about an individual for the purpose of direct marketing.

14. Exception - Personal Information Other Than Sensitive Information

14.1. The Company may use or disclose personal information (other than sensitive information) about an individual for the purposes of direct marketing if:

(a) the Company collected the information from the individual; and the individual would reasonably expect the Company to use or disclose the information for that purpose; or

(b) the Company has collected the information from a third party; and either:

(i) the Company has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or

(ii) it is impracticable for the Company to obtain the individual's consent; and

(c) the Company provides a simple way for the individual to opt out of receiving direct marketing communications from the Company;

(d) each direct marketing communication with the individual the Company:

(i) includes a prominent statement that the individual may make such a request; or

(ii) directs the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made a request to opt out of receiving direct marketing.

15. Exception - Sensitive Information

15.1. The Company may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

16. Requests to Stop Direct Marketing

16.1. Where the Company uses or discloses personal information about an individual for the purposes of direct marketing by the Company or facilitating direct marketing by another organisation, the individual may request:

(a) that the Company no longer provide them with direct marketing communications;

(b) that the Company does not use or disclose the individual's personal information for the purpose of facilitating direct marketing by another organisation;

(c) that the Company provides the source of the personal information.

16.2. Where the Company receives a request from an individual under section 16.1, the Company will:

(a) give effect to the request under section 16.1(a) or 16.1(b) within a reasonable period after the request is made and free of charge; and

(b) notify the individual of the source of the information, if the individual requests it, unless it is impracticable or unreasonable to do so.

16.3. This sections 13-16 do not apply to the extent that the following laws apply:

(a) the Do Not Call Register Act 2006;

(b) the Spam Act 2003; or

(c) any other Act of the Commonwealth of Australia.

17. Disclosing Personal Information to Cross Border Recipients

17.1. Where the Company discloses personal information about an individual to a recipient who is not in Australia and who is not the Company or the individual, the Company must ensure that the overseas recipient does not breach the Australian Privacy Principles (with the exception of APP1).

17.2. The countries we may disclose an individual's personal information to include:

(a) Australia and New Zealand and countries in which Automic Pty Ltd ACN 152 260 814, Kestrel's fund registry and administration services prover, may have an APP or affiliate and transfers Personal Information in compliance with Australian Law.

17.3. Section 17.1 does not apply where:

(a) the Company reasonably believes that:

(i) information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the Company has informed the individual that if they consent to the disclosure of information the Company will take reasonable steps to ensure the overseas recipient does not breach the Australian Privacy Principles; and

(ii) after being so informed, the individual consents to disclosure;

(c) the disclosure of the information is required or authorised by or under an Australian law or a Court/Tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A (1) Privacy Act) exists in relation to the disclosure of the information by the Company.

18. Adoption of Government Related Identifiers

18.1. The Company must not adopt a government related identifier of an individual as its own identifier unless:

(a) the Company is required or authorised by or under an Australian law or a Court/Tribunal order to do so; or

(b) the identifier, the Company and the circumstances of the adoption are prescribed by regulations.

19. Use or Disclosure of Government Related Identifiers

19.1. Before using or disclosing a government related identifier of an individual, the Company must ensure that such use or disclosure is:

(a) reasonably necessary for the Company to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) required or authorised by or under an Australian law or a Court/Tribunal order; or

(d) within a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A (1) Privacy Act; or

(e) reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) the identifier, the Company and the circumstances of the adoption are prescribed by regulations.

20. Quality of Personal Information

20.1. The Company will ensure that the personal information it collects and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

21. Security of Personal Information

21.1. The Company will ensure that it protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.

21.2. The Company will take reasonable steps to destroy or de-identify any personal information it holds where:

(a) the Company no longer needs the personal information for any purpose for which the information may be used or disclosed by the Company;

(b) the information is not contained in a Commonwealth record;

(c) the Company is not required to retain that information under an Australian law, or a Court/Tribunal order.

22. Storage of Personal Information

22.1. The Company stores personal information in different ways, including:

(a) hard copy on site at the Company's head office; and

(b) electronically secure data centres which are located in Australia and owned by either the Company or external service providers.

22.2. In order to ensure the Company protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure, the Company implements the following procedure/system:

(a) access to information systems is controlled through identity and access management;

(b) employees are bound by internal information securities policies and are required to keep information secure;

(c) all employees are required to complete training about information security; and

(d) the Company regularly monitors and reviews its compliance with internal policies and industry best practice.

23. Access

23.1. The Company must give an individual access to the personal information it holds about the individual if so requested by the individual.

23.2. The Company must respond to any request for access to personal information within a reasonable period after the request is made.

23.3. The Company must give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so and must take such steps as are reasonable in the circumstances to give access in a way that meets the needs of the Company and the individual.

23.4. The Company must not charge an individual for making a request and must not impose excessive charges for the individual to access their personal information.

24. Exceptions

24.1. The Company is not required to give an individual access to their personal information if:

(a) the Company 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; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access if frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the Company and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal intentions of the Company in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a Court/Tribunal order; or

(h) the Company has reason that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the Company in connection with a commercially sensitive decision-making process.

25. Refusal to Give Access

25.1. If the Company refuses to give access in accordance with section 24 or to give access in the manner requested by the individual, the Company will give the individual a written notice that sets out:

(a) 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

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

25.2. Where the Company refuses to give access under section 24.1(j) the Company may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

26. Correction of Information

26.1. The Company must take reasonable steps to correct all personal information, having regard to the purpose for which the information is held where:

(a) the Company is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(b) the individual requests the Company corrects the information.

26.2. Where the Company corrects personal information about an individual that the Company previously disclosed to another APP entity and the individual requests the Company to notify the other APP entity of the correction, the Company must take reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

27. Refusal to Correct Information

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

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

28. Request from a Client to Associate A Statement with Their Information

28.1. If:

(a) the Company refuses to correct personal information as requested by the individual; and

(b) the individual requests that the Company associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information,

the Company must take such steps as are reasonable in the circumstances to associate the statement (as described in section 28.1(b) 28.1(b)) with the individual's personal information. The statement should be associated with the information in such a way that will make the statement apparent to users of the information.

29. Dealing with Requests

29.1. The Company must:

(a) respond to requests under sections 26-2829 within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.

30. Complaints

30.1. The Company offers a free internal complaint resolution scheme to all customers. Should a client have a privacy complaint, they are to contact the Company to discuss their concerns using the following contact details:

(a) Email: info@kestrelcapital.com.au

(b) Post: GPO Box 4311, Sydney NSW 2001

30.2. To assist the Company in helping customers, the Company asks customers to follow a simple three-step process:

(a) gather all supporting documents relating to the complaint;

(b) contact the Company to review your situation and if possible, resolve your complaint immediately; and

(c) if the matter is not resolved to the customer's satisfaction, customers are encouraged to contact the Company's Complaints Officer using the details in 30.1.

30.3. The Company will rectify any breach if the complaint is justified and takes necessary steps to resolve the issue.

30.4. In certain situations, to deal with a complaint it may be necessary to consult with third parties. However, any disclosure of Personal Information to third parties will be provided with the customer's authority and consent.

30.5. After a complaint has been received, the Company sends the customer a written notice of acknowledgement setting out the process. The complaint is investigated, and the decision sent to the customer within thirty (30) days unless the customer has agreed to a longer time. If a complaint cannot be resolved within the agreed time frame or a decision could not be made within thirty (30) days of receipt, a notification will be sent to the customer setting out the reasons and specifying a new date when the customer can expect a decision or resolution.

30.6. If the customer is not satisfied with the Company's internal privacy practices or the outcome in respect to complaint, the customer may approach the OAIC with their complaint:

Office of the Australian Information Commissioner

Address: GPO Box 5218, Sydney NSW 2001

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Website: oaic.gov.au

31. Notifiable Data Breaches Scheme

31.1. Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* ("**Privacy Amendment Act**") the Company is required to notify the Office of the Australian Information Commissioner ("**OAIC**") in relation to all eligible data breaches.

31.2. The Company must notify the OAIC by lodging a Notifiable Data Breach Form soon as practicable. The Notifiable Data Breach Form is available at the following link: https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB.

31.3. Under the Privacy Amendment Act, the Company must also promptly inform clients whose personal information has been compromised by the eligible data breach that a breach of their personal information has occurred.

32. Policy Breaches

32.1. Breaches of this Policy may lead to disciplinary action being taken against the relevant party, including dismissal in serious cases and may also result in prosecution under the law where that act is illegal. This may include re-assessment of bonus qualification, termination of employment and/or fines (in accordance with the Privacy Act).

32.2. Staff are trained internally on compliance and their regulatory obligation to the Company. They are encouraged to respond appropriately to and report all breaches of the law and other incidents of non-compliance, including the Company's policies, and seek guidance if they are unsure.

32.3. Staff must report breaches of this Policy directly to the board or its delegate.

33. Retention of Notifiable Data Breach Forms

33.1. The Compliance Officer will retain the completed Notifiable Data Breach Forms for seven (7) years in accordance with the Company's Document Retention Policy. The completed forms are retained for future reference and review.

33.2. As part of their training, all staff are made aware of the need to practice thorough and up to date record keeping, not only as a way of meeting the Company's compliance obligations, but as a way of minimising risk.

34. Policy Review

34.1. The Company's Privacy Policy will be reviewed on at least an annual basis by the Compliance Officer of the Company, having regard to the changing circumstances of the Company. The Compliance Officer will then report to the Director on compliance with this Policy.

Issued by Kestrel Capital Pty Limited

November 2023