DATA AND INFORMATION POLICY

1. What is Information Management?

1.1. Information Management is the handling of datum either discretely (as data) or collated (as information). Data are facts and statistics collected together for reference or analysis. Information is datum organised to have meaning about a specific topic (such as a client).

1.2. There are minimum standards for information management set out in the Lawyers and Conveyancer's Act 2006, the Privacy Act 1993 and in the firm's Client Care Statement.

1.3. Information as a whole, and the way we use data specifically, is what this firm's business model is based upon. The practice of law itself relies heavily on accurate, discreet and succinct communication of information.

2. Why is an Information Management Policy needed?

2.1. To ensure that all clients are treated consistently.

2.2. We have legal and ethical responsibilities to uphold relating to how we treat the personal information of our clients.

2.3. We must show external interested parties (e.g., insurance company, NZ Law Society) that we have considered issues around information management.

2.4. To enable the firm to deliver high-quality legal services at long distance.

2.5. To support clients who would otherwise have difficulty accessing justice due to physical, emotional or locational vulnerabilities.

2.6. To show agreement by all employees on the best way to manage information within the firm.

2.7. To protect the competitive advantages of the firm, namely our reputation for discretion, honesty and innovation.

2.8. Staff time is limited and consideration must be given before creating, changing or deleting diary entries.

2.9. So all employees agree on what is the best way to manage their own and each other's diaries.

2.10. This policy ensures consistency across the entire firm.

3. Procedures governed by this Policy

3.1. The following procedures and related documents are governed by this Policy:

- PRSUP-501.01 Information Management Procedure
- PRSUP-501.02 Diary Procedure
- PRSUP-501.03 Filing Documents in Court Procedure
- PRSUP-501.04 Telephone Enquiry Procedure
- PRSUP-501.05 File Closure Procedure
- GUSUP-501.01A Document Naming Guidelines
- GUSUP-501.01B Public Email Inboxes Guidelines
- GUSUP-501.01A JEMIMA Usage Guidelines
- GUSUP-501.01D Cuckoo Hole Guidelines
- GUSUP-501.01E Server Credential Guidelines
- GUSUP-501.01F Cyber Security Guidelines
- FOSUP-001A Equipment Issue Form
- DOSUP-501.01 User Access Register

4. Commitment to Te Tiriti o Waitangi and a bicultural Aotearoa/New Zealand

4.1. Ebborn Law is committed to the principles of Te Tiriti o Waitangi and the spirit of partnership between Māori and non-Māori. These principles must be used to inform any interpretation of this procedure.

5. Commitment to the United Nations Women's Empowerment Principles

5.1. Ebborn Law is committed to the UN WEPS. These principles must be used to inform any interpretation of this procedure.

6. Key principles

6.1. Special consideration must be given to confidentiality and privacy issues, and the correct identification of clients.

6.2. Compliance to AML/CFT must be observed.

6.3. The principles outlined in the Privacy Act apply at all times. It is each individual staff member's personal responsibility to understand those principles and apply them with scrupulous attention.

6.4. Clients have an inalienable right to information we store about them (except in specific circumstances) and to have that information corrected if it is wrong.

- exceptions must be made in circumstances where the law prevents release of personal information, or the Court has suppressed or sealed information (e.g. psychology report).

6.5. All breaches of this policy <u>must</u> be reported – immediately and without delay – to the Operations Manager in the first instance or to the CEO. This is to allow a decision to be made about whether to report the breach to our insurers and the client.

6.6. This Policy adopts the Principles for Managing Data and Information held by the New Zealand Government [CAB Min (11) 29/12] – amended for use within a law firm – which state that information and data must be:

- open;
- protected;
- readily available;
- trusted and authoritative;
- well managed;
- reasonably priced, and;
- reusable.

6.7. Diary appointments must be within the staff member's normal working hours.

6.8. Some types of appointments may be entered on any day, others are limited to certain days.

6.9. Diary entries must realistically reflect the actual time-cost of an appointment.

6.10. A diary is part of the firm's record and appointments must never be deleted except in special circumstances.

6.11. Staff who use artificial intelligence-enabled tools for work purposes must have a comprehensive understanding of the workings of AI and large language models, including the risks posed by AI and any guidelines issued by the Courts of New Zealand[1].

7. Open

7.1. Client data and information held by Ebborn Law should be open for that client's access unless grounds for refusal or limitations exist under the Lawyers and Conveyancers Act or Court rules. In such cases they should be protected.

8. Protected

8.1. Personal, confidential[2] and privileged[3] data and information are protected.

9. Readily Available

9.1. Open client data and information are released proactively and without discrimination. They are at all times discoverable and accessible by the client via a staff member.

10. Trusted and Authoritative

10.1. Data and information support the purposes for which they were collected and are accurate, relevant, timely, consistent and without bias in that context.

[1] Courts of NZ, (2023). *Guidelines for use of Generative Artificial Intelligence in Courts and Tribunals (Lawyers)*

2 Confidential client information is limited in how and to whom it is distributed (such as reports ordered under s132 and s133 of the Care of Children Act)

3 Privileged information may legally be not released to anyone other than the client (due to lawyer-client privilege) unless statutory exceptions apply

10.2. An entire client file released to the client on request must contain – with the **strict exception** of the 7 CONFIDENTIAL folder – all data and information, regardless of any implications for the firm. A client file will include, *inter alia*:

- Hardcopy documents (if requested) with the exception of confidential documents
- Electronic documents, including drafts, with the exception of confidential documents
- File notes
- Emails relating to the client, but not internal emails between Ebborn Law staff unless particularly relevant to the case (these should have been placed in the client's email folder)
- Note that files in the 7 CONFIDENTIAL folder are not to be released to the client

11. Well Managed

11.1. Client data and information held and owned by Ebborn Law:

- belong to the client;
- are a core asset held by Ebborn Law as a steward on behalf of the client;
- should only be collected or generated for specified and adopted public policy, operational business, or legal purposes, and;
- will be managed in keeping with the Privacy Principles as outlined in s22 of the Privacy Act 2020.

11.2. Staff are stewards of Ebborn Law-held client data and information, and must observe good practices which manage the data and information over their life cycle, including catering for technological obsolescence and long-term preservation and access. Good practices also include collaborating with other staff, support agencies and the client; facilitating access; strengthening awareness, and; supporting cooperation with government agencies.

11.3. All data and information held by Ebborn Law on behalf of clients must be kept secure from theft, tampering or disclosure.

11.4. Ebborn Law operates a paperless office. Where possible documentary information should be returned into the care of client (aside from documents held on behalf of a client such as wills, EPOAs, relationship agreements, etc.).

11.5. Any theft, tampering or disclosure must be brought to the attention of the client and Chief Executive Officer without delay and the firm's insurer - and where appropriate the Office of the Privacy Commissioner - must be fully informed.

11.6. All client information must be retained for seven (7) years before being securely destroyed (the exception is current wills and deeds, which should not be destroyed).

11.7. Client information that is not required to be at-hand (closed files) must be archived securely.

11.8. The closure, archiving, transfer and release of client information must be recorded in an auditable fashion.

11.9. Staff must implement these practices on a day-to-day basis.

12. Privacy Principles

12.1. Principle 1 – We will only collect information if it is necessary for a lawful purpose, bearing in mind:

- if the lawful purpose for which personal information about an individual is collected does not require the collection of an individual's identifying information, we may not require the individual to produce identification;
- this is particularly relevant to AMLCFT Act requirements that the firm is required to undertake.

12.2. Principle 2 – Any personal information must be collected from the individual concerned. Exceptions may be made but these must be specified in procedures, guidelines or SOPs, or authorised in writing by the CEO.

12.3. Principle 3 – Individuals that we collect information from must be made aware of:

- the fact that the information is being collected;
- the purpose for which the information is being collected;
- the intended recipients of the information;
- the name and address of the agency that is collecting the information;
- the agency that will hold the information;
- if the collection of the information is authorised or required by or under law, then the particular law by or under which the collection of the information is authorised or required;
- whether the supply of the information by that individual is voluntary or mandatory;
- the consequences (if any) for that individual if all or any part of the requested information is not provided; and

- the rights of access to, and correction of, information provided by the Privacy Principles.

12.4. Principle 3A – Where personal information is collected from a source other than the individual concerned, the firm must take any steps that are reasonable in the circumstances to ensure that the individual concerned is aware of:

- the fact that the information has been collected;
- the purpose for which the information has been collected;
- the intended recipients of the information;
- the name and address of the agency that has collected the information;
- the agency that will hold the information;
- if the collection of the information is authorised or required by or under law, then the particular law by or under which the collection of the information is authorised or required;
- whether the supply of the information by the individual is voluntary or mandatory if collected directly from that individual;
- the consequences (if any) for that individual if all or any part of the information is not provided; and
- the rights of access to, and correction of, information provided by the Privacy Act 2020.

Notification must be provided as soon as reasonably practicable after collection unless an exception[4] applies under Information Privacy Principle 3A and Schedule 2 of the Privacy Act 2020. Staff must consult the Privacy Officer before relying upon an exception to notification.

12.5. Principle 4 – Information about an individual must be collected lawfully and fairly and does not intrude up the personal affairs of the individual.

12.6. Principle 5 – The firm will take all reasonable action to protect personal information held on behalf of individuals.

12.7. Principle 6 – All information held by the firm is the property of the client, with the exceptions listed below. information held about other individuals (who are not clients of the firm) is restricted under Rule 5.1 of the Lawyers and Conveyancers Act (Lawyers: Conduct and Client Care) Rules 2008 (RCCC) and as such may be withheld as per s53(d) of the Privacy Act 2020.

The following are not property of the client:

- documents and information prepared for the benefit of the lawyer or the firm, including *aide memoir*, forms used for internal administrative purposes, bank account statements relating to monies held for the client, transaction or reporting records, etc.;
- documents or communication relating to reporting under the Anti Money Laundering and Countering the Financing of Terrorism Act;
- documents or information relating to cyber security or legal relationships with third parties (such as non-disclosure agreements or contracts).

12.8. Principle 7 – Any individual may request the firm corrects any information held about them. Such request is decided by the Privacy Officer. Denial of a request must result in the original request being held on file along with the justification for refusing the change(s).

12.9. Principle 8 – Personal information must not be used or disclosed without certainty the information is accurate, up-to-date, complete, relevant and not misleading.

12.10. Principle 9 – Personal information must not be kept beyond the use of its lawful purpose. After an effort to contact the client to offer their return, matter files may be securely disposed of after a period of ten years with the exception of documents evidencing legal obligation (contracts, wills and deeds), which must be kept in perpetuity or until claimed by a client or estate.

The relationship between solicitor and client is essentially a contractual one and there is no requirement in law to retain documents. The client care statement provided to all clients forms part of the retainer (contract) with the firm and this stipulates documents will be securely destroyed after ten (10) years.

Rule 4.4.1 of the Conduct and Client Care Rules specifies that the client has the right to uplift all documents held on the client's behalf when changing lawyers. As the Rules don't specify which documents are held on 'behalf', the firm's policy is that all personal information (including documents) held are the property of the client as per Principle Six, with the exceptions mentioned.

Documents containing personal information that is not required to be retained and where there is also no need to retain must be securely destroyed immediately.

[4] Refer to Appendix A for a list of exceptions

Rule 11(5) of the Lawyers and Conveyancers Act (Trust Account) Regulations 2008 require that trust account records relating to a client are retained for a period of at least six (6) years from the date of the last transaction recorded in them.

Authority and Instruction Forms relating to eDealing transactions are required to be retained for a period of at least 10 years from the date on which the instrument is lodged for registration (Land Transfer Regulations 2002, reg 14; NZLS Guidelines for the use of Landonline for an electronic transaction, guideline N).

Under the Limitation Act 2010 money claims are subject to a limitation period of 6 years from the date of the act or omission on which the claim was based. S 11(3) of the Act provides for an extension of three years following discovery of the relevant facts in certain cases where the plaintiff was not aware of all aspects of the claim. The maximum limitation period is 15 years following the act or omission relied on.

Opinion obtained by the New Zealand Law Society advises retention of documents for ten (10) years.

12.11. Principle 10 – Personal information may not be used by the firm for any other purpose aside from that for which it was obtained, unless in doing so the individual cannot be identified in any way or it is allowed under s22 of the Privacy Act 2020.

12.12. Principle 11 – Personal information must not be disclosed to any other person or agency unless it is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained, or if the individual has given specific permission to release the information, or if the firm is required under law to release the information.

12.13. Principle 12 – Personal information may not be released to any foreign person or entity without express written authority of the Privacy Officer and Principal Lawyer.

12.14. Principle 13 – Any personal unique identifier (PUI) not originating from the firm must not be retained unless there is a specific legal requirement, and any PUI on a document provided by a client must be permanently redacted.

- Obvious exceptions include: court numbers; legal aid numbers; Police or Oranga Tamariki file reference numbers where necessary for the execution of a lawyer's duties.
- Documents that must have PUIs redacted include: any form of identity document.

13. Reasonably Priced

13.1. Use and re-use of Ebborn Law-held client data and information is expected to be free. Charging clients for access is discouraged.

13.2. Pricing to cover the costs of dissemination is only appropriate where it can be clearly demonstrated that this pricing will not act as a barrier to the use or re-use of the data. If a charge is applied for access to data, it should be transparent, consistent, reasonable, justifiable and the same cost to all clients.

14. Reusable

14.1. Data and information are released:

- with the highest possible level of granularity;
- in re-usable, machine-readable format, and;
- in an easily-transportable and accessible form according to the client's needs.

15. AML/CFT

15.1. Privileged information[5] may be released to the Commissioner of Police and any other party permitted under the Anti-Money Laundering and Countering of Financing of Terrorism Act 2018 by the firm's AML/CFT supervisor[6].

15.2. Information relating to the firm's suspicion of money laundering, or financing of terrorism, may and <u>must</u> be withheld from the client for the process of enabling law enforcement and related agencies to undertake investigations[7].

15.3. When engaging with a client using VLaw® there must be consideration toward any risk inherent in not meeting with the client in person, with regards to money laundering or the financing of terrorism.

[5] AMLCFT Act 2018 s42(2)

[6] ibid. s48

[7] ibid. s46(2)

16. VLaw®

16.1. VLaw® is a registered trademark of The Essential Admin Co Ltd. It is a unique means of delivering law services over distance, rather than face-to-face. It is undertaken over video link and can use additional technology such as scanners, telephones, SMS text messaging, and printers.

16.2. Whilst any client is potentially able to use the VLaw® system, preference should be given to:

- people who cannot access a lawyer due to physical or emotional vulnerability
- people on remand or in prison
- people who live in areas where there are reduced numbers of family legal aid providers

16.3. Clients must have access to video and audio transmission equipment and a suitably high-speed internet connection (VDSL is acceptable, fibre is preferred).

16.4. In some instances Ebborn Law will have agreements with specific agencies or organisations to provide VLaw® services to their clients.

17. Responsiveness

17.1. Guiding principles for responsiveness are:

- Our values drive our need to be responsive to enquiries.
- The Lawyers and Conveyancers Act requires the firm to respond in a timely manner to queries from clients and Counsel.
- The firm's clients are referred on a word-of-mouth basis. If we gain a reputation for responsiveness, it will boost our reputation and thus the number of clients.

17.2. Timeframes for response:

- The phone must be answered immediately if possible. If not possible, the messages should be checked as soon as practicable.
- Phone messages must be responded to in a timeframe appropriate to the enquiry, but no later than 24 working hours (for example if a phone message is left on Friday at 3 p.m. then it must be responded to by 3 p.m. the following Monday).
- Email communications must be responded to within 24 working hours.
- Postal mail communications must be responded to within five (5) working days:
- If the response is complex (for example, requires research or communication with an external agent) then a letter of acknowledgement must be sent within five (5) working days and a follow-up letter in answer must be sent within 15 working days.

17.3. If for some reason it is not possible to respond to a communication within the timeframes then a file note must be made on the matter file, or the Operations Manager must be informed.

17.4. Response to a communication should be made using the same method it was sent to the firm, if practicable. For example, a text message received should get a text message back. Exceptions can be made if there is a valid reason (for example, if the response to a text message is highly complicated and requires a voice call or a letter).

17.5. Employees or contractors who are told by a person that their query has not been responded to must:

- Email the staff member who the person says has been unresponsive, telling them the person has complained about non-responsiveness, and;
- Copy in complaints@ebbornlaw.co.nz to the email; and
- Make a file note on Jemima if practicable.

Note: Complaints are treated as an opportunity to improve ourselves and should not be used negatively toward a staff member. In many cases miscommunication can occur through no fault, or from the fault of the client, or from simple misunderstanding. We never seek to lay blame; we always seek to learn how to improve.

18. VLaw® case management

18.1. Clients must advise staff members if there is another person/people in the room off camera.

18.2. Aside from a screen shot to obtain proof of identity, at no time may a recording be made of the video, audio or screenshot of the client unless in specific situations outlined in the procedures and with the client's express written consent (for example, using Contented AI to assist with the interview process/document generation).

18.3. Case management appointments will be conducted in advance of any legal services provided and funding secured as per company policy, the exception being urgent cases.

19. VLaw® legal services

19.1. Clients must advise lawyers if there is another person/people in the room off camera.

19.2. VLaw® clients will receive the same standard of legal services as any client of Ebborn Law.

19.3. Some matters are not suitable for VLaw®. These include wills, relationship property or enduring powers of attorney.

20. Artificial intelligence

20.1. Before using any artificial intelligence tool for work purposes, staff must ensure they have a sound understanding of the tool's capabilities and limitations.

20.2. Staff should not enter any information into an AI-enabled tool not approved by the Privacy Officer that is not already in the public domain: in particluar information that is private, confidential, suppressed or legally privileged.

20.3. Lawyers are responsible for ensuring that all information they provide to the court/tribunal is accurate. It is the responsibility of the lawyer to check the accuracy of any information generated by an AI-enabled tool (including legal citations) before using that information in court/tribunal proceedings. Note that the Supreme Court has indicated that lawyers or clients who falsely cite authorities in documents submitted to court (including hallucinations generated by artificial intelligence) risk committing an obstruction to justice or a contempt of court[8].

20.4. When using AI-enabled tools, staff must always have regard to ethical issues – particularly biases and the need to address them.

20.5. Whilst the courts do not require disclosure of AI use as a matter of course, it has been the policy of the firm for some time to disclose whether or not any information provided to the court in a client affidavit/affirmation has been generated by AI or altered in any way.

21. Compliance

21.1. Staff of Ebborn Law (Portia) are bound by their individual employment agreements and the firm's Code of Conduct to keep all data and information of the firm (including client information) safe. This is also a requirement of the Lawyers and Conveyancers Act 2006[9] to protect client information.

21.2. Breach of privacy caused by honest human error shall always be treated as a learning opportunity without any application of blame. This is to remove any barrier to reporting a breach that might be caused by a fear of authority.

21.3. Any intentional breach of firm policy or procedure that leads to a breach of privacy or a cybersecurity incident will be treated as serious misconduct (allowing unauthorised access to, or disclosure of any matter or information in relation to Ebborn Law business).

21.4. Any intentional breach of firm policy or procedure that creates a risk of, or could lead to, a breach of privacy or a cybersecurity incident will be treated as Misconduct (negligence or carelessness in the performance of duty; failure to comply with a lawful instruction, including a reasonable and lawfully given warning, unless there is good and sufficient cause to do otherwise).

22. Complaints

22.1. Any complaints must be handled according to *POLEG-602 - Service Delivery Policy* and *PRLEG-602.01 - Complaint Investigation Procedure*.

23. Privacy and confidentiality

23.1. All information that relates to client matters or Court activities are private and confidential and must be treated as such. At no time will information we hold on behalf or about clients be disclosed unless we are required to do so by law or – if allowed under legislation and other various covenants – where it is necessary to do so to provide our services to the client or when requested by the client or with their consent.

---

8 Jones v Smith [2025] SC 167, [2026] 1 NZSC 3 at [7]

9 rule 8 of the RCCC, which provides that lawyers have a duty to protect and hold in strict confidence all information concerning: a client, the retainer, and the client's business and affairs.

APPENDIX A

Exceptions to Privacy Principle 3A

1. The individual already knows: The agency reasonably believes the individual is already aware of the matters that would otherwise need to be notified.
2. Compliance is not reasonably practicable: The agency cannot reasonably provide the notification, for example because the individual cannot be located or the effort required would be disproportionate.
3. Non-compliance is authorised by the individual: The individual has authorised the agency not to provide the notification.
4. Notification would prejudice the purposes of collection: Providing the notification would undermine the purpose for which the information was collected (e.g. certain investigations into misconduct or fraud)
5. Notification would prejudice enforcement activities: Notification would prejudice the prevention, detection, investigation, prosecution, or punishment of offences.
6. Notification would prejudice the protection of public revenue: For example, certain tax compliance investigations.
7. Notification would prejudice the conduct of court proceedings: Where notification would interfere with existing or contemplated legal proceedings.
8. Information collected for statistical or research purposes: Where the information will not be published in a form that identifies individuals.
9. Notification would prejudice the physical or mental health of the individual: Or another person's health, safety, or wellbeing.
10. Notification would disclose the affairs of another individual: Where notifying one person would improperly reveal another person's personal affairs.
11. Information collected under a lawful authority for intelligence, security, or similar functions: Certain public sector agencies may rely on specific statutory powers.
12. Maintenance of the law exception: Certain law enforcement and regulatory functions may justify non-notification.

SCHEDULE ONE

Version Control Table

Version	Date	By	Changes	Page
1.0	24/03/15	JC	Initial draft	n/a
2.0	28/09/20	JC	Updated format	various
2.1	14/10/20	JC	Added clauses 4.7-4.10 (use of diary)	3
2.2	25/10/22	JC	Added clause 14 (responsiveness)	5
2.3	27/07/23	JC	Added reference to privacy principles (clause 9.1) Added clause 10 (privacy principles)	3 4
2.4	18/02/26	JC	Grammatical corrections Updated clause 3 (documents subsidiary to this policy) Added TOW clause Added WEPS clause Added clause 6.11 (key principles around artificial intelligence) Added clause 20 (policies around use of artificial intelligence tools) Corrected clause 21.1 (*Service Delivery Policy*) Added Version Control Table	various 2 2 2 3 7 8 9
2.5	05/06/26	JC	Changed principle titles in clause 12 to number format (from written format) Added clause 12.3 (Principle 3A) Renumbered clauses subsequent to 12.3 Added clause 21 (Compliance) Renumbered clauses subsequent to 21 Added Appendix A (exceptions to IPP3A)	4,5 5 5 8 8,9 10
2.6	26/06/26	JC	6.5 now shows breach reporting lines to Operations Manager and CEO 10.2 now reflects that confidential information is not to be released to a client 11.6 changed from ten (10) years retention to seven (7) years 16.1 removed reference to fax machines 17.2 timeframe for response to emails changed to 24 hours, consistent with phone calls 17.3 changed Practice Manager to Operations Manager 18.1 removed reference to LRT 18.2 added exampled of when recordings may be made with client consent 18.4, 18.5, 18.6 removed	3 4 4 7 7 7 7 7 8