Privacy Statement for

Section 1

Glossary

Acronym	Short for
the Act	Privacy Act 2020
PO	Privacy Officer
IPP's	Information Privacy Principles
the AML/CFT Act	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
The Company	New Zealand Family Trust Services Limited, New Zealand Foreign Trust Services Limited

Table of Contents

GLOSSARY 1

SECTION 1 4

GENERAL INTERPRETATION 4

PRIVACY OBJECTIVES 4

RESPONSIBILITIES 4

WHO IS RESPONSIBLE 4

SUPPLIER DETAILS 5

TRAINING 5

DOCUMENTS 5

SECTION 2 5

IPP'S 6

IPP 1 – COLLECTION OF INFORMATION 6

IPP 2 – SOURCE OF INFORMATION 6

IPP 3 – COLLECTION OF INFORMATION FROM THE INDIVIDUAL 7

IPP 4 – MANNER OF COLLECTION OF INFORMATION 8

IPP 5 – STORAGE AND SECURITY OF INFORMATION 9

IPP 6 – ACCESS TO INFORMATION 11

IPP 7 – CORRECTION OF INFORMATION 12

IPP 8 – ACCURACY OF INFORMATION 14

IPP 9 – DELETION OF INFORMATION 14

IPP 10 – USE OF INFORMATION 15

IPP 11– DISCLOSURE OF INFORMATION 16

IPP 12– DISCLOSING INFORMATION OUTSIDE NEW ZEALAND 17

IPP 13– UNIQUE IDENTIFIERS 18

SECTION 3 19

BREACH NOTIFICATIONS 19

COMPLIANCE NOTICES 21

WEBSITE PRIVACY STATEMENTS 22

APPENDIX I – TECHNOLOGY SECURITY 25

Section 1

General interpretation

The context otherwise requires, references to “we”, “us” and “our” are references to New Zealand Family Trust Services Limited including its staff, successors and all Delegated Parties.

Privacy Objectives

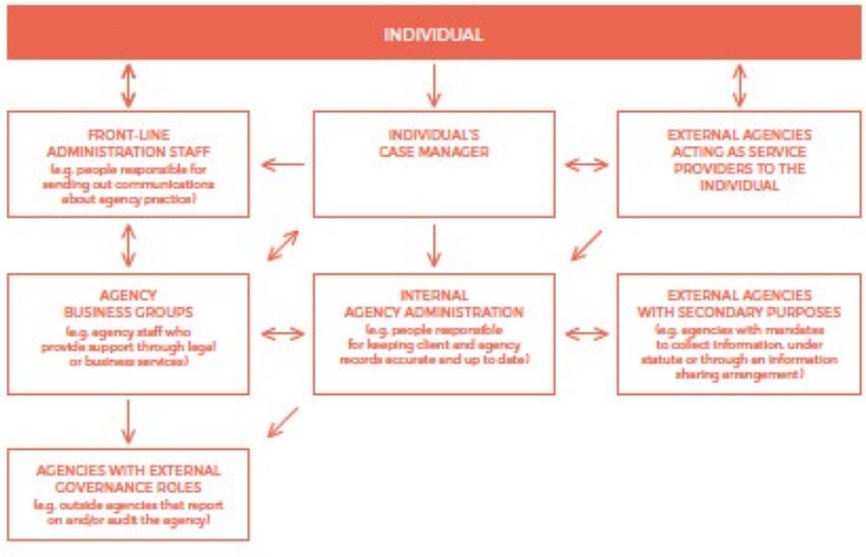
Under the Act individuals and companies are required to establish policies and safeguards to ensure the privacy and security of client information.

We are committed to ensuring all our policies and processes (and the technology we use to support our processes) not only comply with all relevant legislation but also meet public expectations and to ensure they are effectively implemented. This commitment covers our policies and processes for collecting, using, storing, keeping safe, and disposing personal and other confidential information. The following information outlines how we will ensure compliance with the Act.

Responsibilities

It is the responsibility of management and all staff to ensure that all areas of the Act are being adhered to.

As noted below there are many touch points as it relates to client information and all areas must be considered.



Who is responsible?

The following outlines expectations of our various staff:

Directors

1. Overall overseeing of all privacy related issues in conjunction with the PO.
2. Overseeing the privacy policy framework in conjunction with the PO to ensure compliance.
3. Sign off on the Privacy Statement document to show commitment.
4. Communication to any staff on what is expected of them in their various roles.

Privacy Officer

1. Be familiar with the privacy principles in the Act
2. Work to make sure the organisation complies with the Act
3. Deal with any complaints from the organisation's clients about possible privacy breaches

4. Deal with requests for access to personal information, or correction of personal information

5. Act as the organisation's liaison with the Office of the Privacy Commissioner.

6. Liaise with the director/s on a regular basis to inform them of any issues that relate to privacy.

They may also:

1. Train other staff at the organisation to deal with privacy matters.

2. Advise their organisation on compliance with privacy requirements.

3. Advise their organisation on the potential privacy impacts of changes to the organisation's business practices.

4. Advise their organisation if improving privacy practices might improve the business.

5. Be familiar with any other legislation governing what the organisation can and cannot do with personal information.

Administration

Understand the principles, policies, and procedures relating to the security and management of confidential information within the Company.

1. Apply these as appropriate to their role.

2. Report breaches, incidents, and near misses to the security and privacy teams.

3. Control and provide education about correct management, retention, and disposal of confidential information in accordance with the Act and other regulations.

Frontline staff

Understand the principles, policies, and procedures relating to the security and management of confidential information within the Company and how that applies to the direct dealings with clients.

Supplier details

The following is a list of suppliers used in the services provided where personal information may be supplied:

IT – Terminal Server supplied by CNS

Website: JFM Creatives

E-mails: Freeparking

The privacy policies of each of the suppliers has been checked by the PO as per the contracts on file. Any new contracts will be checked for privacy issues and signed off by the PO before signing by the director/s.

Training

The Companies are operated by the two directors and have two part time contractors. Training of the contractors is to be actioned by the directors of the Companies and will sign off that this has been actioned.

Documents

All client facing documents have been checked by the PO to ensure they comply with the Privacy principles and the Act and have been signed off by us.

Any future changes to any of the company’s documents are to be vetted by our compliance consultant and the PO and signed off by the directors. This will also include any other regulatory changes that occur in the future which is the responsibility of the PO.

IPP's

There are 13 principles included in the Act and the following outlines our policy, procedures and controls as it relates to each of the IPP's.

IPP 1 – Collection of Information

Personal information shall not be collected by us unless:

a) the information is collected for a lawful purpose connected with a function or activity of ours; and

b) the collection of that information is necessary for that purpose.

What Principle 1 means in practice

Focused – we will only collect personal information if that is needed. The most effective privacy safeguard is not to collect information in the first place if it is not needed. Good overall information management often stems from being clear about the purpose at the start. For instance, if we are not clear about why we need the information, we will not know who needs to see it, or whether it's being used properly, or how to explain to the individuals concerned what we are doing with the information. It's not enough simply to say that the we might need the information sometime, or that it's easy to collect.

Company requirements

The following is an outline of what information is needed by us to allow us to conduct the services to the clients.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Client Name, DOB, address, phone, E-mail SOW/SOF, PEP status, assets to be included in the trust. This may be in the form of copies of passports, driver's license and other identifying documents including banking details.	The Company uses a "Fact Find" document to obtain all the information needed to establish and administer a trust. In this document page 1 outlines the Act requirements and the AML/CFT requirements. The company obtains verified photo identification and proof of address in hard copy form and is held on client file. Verified SOF/SOW is also required for AML/CFT purposes and is also held on file.	AML/CFT ACT and Trusts Act 2019 Note: This is not a complete list of Acts and regulations. This applies to all of the IPP's noted below.

IPP 2 – Source of Information

Where we collect personal information, we shall collect the information directly from the individual concerned, unless one of the listed exceptions applies.

What Principle 2 means in practice:

When we collect information about someone, we will get it from them directly wherever possible, and the client should also be aware why we need it and what it will be used for. Also, it's often the people themselves who are best placed to provide accurate information.

We can collect information from another source if we believe that one of the exceptions to the principle applies.

These include:

- if the individual concerned has authorised us to collect the information from someone else
- if the information is already publicly available
- if getting it from another source would not prejudice the individual's interests
- if the information will not be used in a way that identifies the individual concerned (including where it will only be used for statistical or research purposes and the individual will not be identified)
- if collecting it from another source is necessary to enforce the law, or for court proceedings, or to protect public revenue, or if collecting it from the individual concerned is not reasonably practicable in the circumstances.

Company requirements

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information which has personal details and ID requirements is needed to abide by AML/CFT regulations and for the establishment and administration of a trust. In some cases where there are other trustees or appointers the information may be supplied by the settlors. As we are dealing in trusts, enhanced CDD for AML/CFT is required which includes SOF/SOW of the settlors.	The Company uses a "Fact Find" document to obtain all the information needed to establish and administer a trust which is completed with the client. In this document page 1 outlines the Act requirements and the AML/CFT requirements. As it relates to information provided for other people there is a sentence noting that information provided is deemed as being authorised by those persons. The company obtains verified photo identification and proof of address in hard copy form and is held on client file. Certified copies may also be obtained where other trustees or appointers are involved. Verified SOF/SOW is also required for AML/CFT purposes and is also held on file. The settlor in most cases will sign off the Fact Find document.	AML/CFT ACT and Trusts Act 2019

IPP 3 – Collection of Information from the Individual

Where we collect personal information directly from the individual concerned, we will take such steps (if any) as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

a) the fact that the information is being collected; and

b) the purpose for which the information is being collected; and

c) the intended recipients of the information

d) the consequences (if any) for that individual if all or part of that information is not provided.

e) the rights of access to, and correction of, personal information provided by these principles.

What Principle 3 means in practice:

In is important to tell people why we need their personal information and what we will do with it.

When information is collected from an individual, whether this is voluntary or compulsory, we need to tell them what it is needed for, and what it is to be used for. If they do not have a choice about giving the information, it is to be spelled out what statutory provisions require them to do this, and any limits on how those provisions can apply.

As with principle 2, there are some exceptions that allow the Company not to spell out what the Company is doing – for instance because it:

- would frustrate the lawful purpose of collecting the information.
- could prejudice a criminal investigation.
- is not reasonably practicable in the circumstances.

Company requirements

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information gathering requirements are as noted in IPP 1 & 2. To inform clients that what the information is for and why.	We use a "Fact Find" document to obtain all of the information needed to establish and administer a trust. In this document page 1 outlines the Act requirements and the AML/CFT requirements. Our letter of engagement document under section 4 also outlines who the information may be provided to and why. Our name and address details are also shown on the Fact Find. Fact Find also states the acts requiring the information along with the letter of engagement.	AML/CFT Act and Trusts Act 2019

IPP 4 – Manner of Collection of information

Personal information shall not be collected by us:

a) by unlawful means; or

b) by means that, in the circumstances of the case,

i) are unfair; or

ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

What Principle 4 means in practice:

We are to be considerate fair and will not be unreasonably intrusive when required to collect information.

Company requirements

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information gathering requirements are as noted in IPP 1 & 2.	All personal information is gathered in the majority of cases on a face-to-face basis with the client and as noted above is done by the way of our Fact Find document that the client signs off.	AML/CFT Act and Trusts Act 2019

IPP 5 – Storage and Security of information

We will hold personal information and shall ensure:

a) that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against

   i. loss; and

   ii. access, use, modification, or disclosure, except with the authority of the Company that holds the information; and

   iii. other misuse; and

b) that if it is necessary for the information to be given to a person in connection with the provision of a service to us, everything reasonably within our power is done to prevent unauthorised use or unauthorised disclosure of the information.

<u>What Principle 5 means in practice:</u>

Take care – keep it safe.

We need to ensure that personal information is protected against misuse, loss or theft. Security is going to be relevant whether maintaining or upgrading an existing database of client information, moving information into a new application or other system, or developing a new business process or access model that changes how personal information is used or who has access to information.

There are some additional things we must also consider which is third party support IT systems or business processes and giving them access to the system that holds the information.

system enforces strong passwords for email accounts, and these are used with your email address to authenticate logins for incoming email, and before sending messages.

Our servers accept encrypted connections from any device you use for email, and this is a default setting on most modern mail software.
It is possible to use an un-encrypted connection, but we advise against it.

<u>Company requirements</u>

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	All documents such as Fact Finds, Letter of Engagements, Clients ID, Trust deeds and auxiliary documents to administer the trusts is required to be kept and appropriate protection around that data held in both hard and electronic form.	Currently the Company operates from a home office and all client hard copy files and software systems are held in the designated office. The security of the hard copy files is via lockable cabinets and alarmed house. Client data is held on a windows terminal server operated by CNS Software. Back up servers are provided by CNS Cloud and are all encrypted. Laptops are bitlocker encrypted. E-mail servers are with Freeparking. The system enforces strong passwords for email accounts, and these are used with your email address to authenticate logins for incoming email, and before sending messages. The servers accept encrypted connections from any device used for email, and this is a default setting on most modern mail software. Only two staff and two part time contractors who have access to the client data in hard and softcopy format which is password protected. Hard copy posting of client details is actioned via courier and normal mail. The personal information is held in various documents as it relates to a trust and deletion of data will be actioned based on the regulations surrounding each document. Where information is to be disposed of this done by way of a commercial destruction service via a secure bin which is	AML/CFT Act and Trusts Act 2019

		commercially collected on a regular basis.	

IPP 6 – Access to Information

Where we hold personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled:

a) to obtain from us confirmation of whether or not we hold such personal information; and

b) to have access to that information

What Principle 6 means in practice:

We must keep people informed – tell them what information we hold.

In most cases, people have a right to access the personal information we hold about them. That means we need a system that enables us to find information about people when they ask and provide it to them.

Our records-management systems must take into account the fact that individuals may wish to access the information we hold about them.

We don't have to hold on to information forever, but while we do have it we should be able to find it – wherever it is (onsite, in archives, offshore, in people's inboxes – or even in our heads).

We must provide a decision about access as soon as reasonably practicable, and not more than 20 working days after the request comes in (unless we have a valid reason to extend this time limit). We also must provide the information itself without undue delay.

Company requirements

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	All personal information required to set up trusts is held in hard and soft copy form and needs to be available if requested from clients.	Any requests for information will be handled by the directors and the PO. All information is readily available from our hard copy files held in the house office filing cabinets. All softcopy information is available via our CNS windows software programme and is always available to obtain. If we get a request from a client to provide their personal information we hold on file, this will go to the director or administration who will enter this into our request information register. This will then be discussed with the PO. A check is made to ensure that the person requesting the information is the person we hold the information on and is not coming from a third party. This is done by phoning the client with the details we have	AML/CFT Act and Trusts Act 2019

		on file to verify a written request. If a verbal request is made a confirmation e-mail is to be sent noting the request and a confirmation must be received before details are released. If we believe there could be a reason not to provide the information as stated under sections 27 to 32 of the Act , we will refer to our lawyer. If accepted, the information will be supplied by giving the requester an opportunity to inspect or have copies made available. Where there may be recordings either visual and/or sound, they will be made available for the requester to hear and or view.	

IPP 7 – Correction of Information

Where we hold personal information, the individual client concerned shall be entitled:

a) to request correction of the information; and

b) to request that there be attached to the information a statement of the correction sought but not made.

<u>What Principle 7 means in practice:</u>

Make it right – let them correct it if we have got it wrong.

If we hold information about an individual that they think is wrong, they are entitled to ask us to correct it.

Sometimes, the person's opinion of what is right may differ from our own. In that case, we do not have to delete or correct the information. However, if the person wants us to, we must add a statement of what the person thinks is correct to your file, in such a way that anyone reading it later will know what that person's view of the information is, as well as our own.

If we correct information, but we have already passed the original information on to another organisation, we will, if possible, notify the other organization that the information has been changed.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	All personal information held on an individual, that individual has the right to correct that information if they believe it to be in inaccurate.	If a request is received to correct information held about them, the director will access this request and ensure that the request has been received by the individual in concern by phoning the client if a written request is received. If it is via voice then an e-mail will be sent to the individual confirming	AML/CFT Act and Trusts Act 2019

		information is being changed. The directors in consultation with the PO will determine if the request to change is in line with what the Company expects. If there is a differing opinion then the directors will make a note on their file noting what requests to change was from the client. Requests will be actioned via the software system where appropriate and additional file notes if this cannot be actioned. The expectation is that this will be actioned within 20 working days from the date of request. If it is deemed that the request may take longer than the 20 days the extension period will be communicated to the requestor. Confirmation to the request will be supplied in writing or via e-mail, which may be a confirmation that the corrections have been actioned or a note to say why the Company will not action the request. If a request is refused one of the directors or PO will advise the requester that they have the right to make a complaint to the commissioner. The director is to analyse if any other third parties need to be informed of the change to ensure the services provided can continue accurately. Clients are made aware of the right to correct information held about them via the Fact Finding document page 1.	

IPP 8 – Accuracy of Information

Where we hold personal information on our clients, we will not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.

What Principle 8 means in practice:

Keep on the mark – ensure it's correct and relevant before you use it.

Poor-quality information could lead to poor decision-making, which in turn may lead to unfair and inappropriate practices and unwarranted adverse effects on the individuals concerned.

Poor data may also make it harder for us to perform our functions efficiently and effectively and meet the clients objectives. Inaccurate or outdated information can be particularly problematic, both for us and the individuals concerned, if we can't get in touch with our clients when we may need to verify their details and circumstances.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	All personal information held on an individual should only be used when that information is believed to be accurate, up to date, complete, relevant and not misleading.	Initial information is collected when trusts are to be established which is signed off by the clients as being accurate and up to date. At the yearly trust meetings which is a requirement, all information is re checked via annual review form along with any new information in the period. All information originally collected is required to ensure the correct administration of the trusts as outlined in the Fact Find. The director and/or PO is to notify any third parties that are used in its service offering, if any data is found to be inaccurate and could affect the ability to act correctly.	AML/CFT Act and Trusts Act 2019

IPP 9 – Deletion of Information

Where we hold personal information, we shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.

What Principle 9 means in practice:

If we have no real reason to keep personal information, we will securely destroy it ("just in case" is not a good enough reason for us to retain information).

Obviously, we can't destroy documents that must be retained under other laws (for instance, to comply with the Public Records Act or Tax Administration Act, Trust Act and AML/CFT Act). However, we need to make sure that any historical documents retained for those purposes are kept secure and can't be accessed by anyone who does not need to see them.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Records must be retained as it relates to various acts, such as the Trust Act and AML/CFT Act. In most cases this is a period of 7 years for certain information but in the case of trusts can be longer.	All records are dated and where a client ceases services with the Companies these are checked periodically to see if these records should be destroyed via a secure destruction service for hard copy information. The internal software system is also checked at the same time and information deleted where appropriate.	AML/CFT Act and Trusts Act 2019

IPP 10 – Use of Information

Where we hold personal information that was obtained in connection with one purpose, we shall not use the information for any other purpose unless we believe, on reasonable grounds, a specified exception apply.

What Principle 10 means in practice:

We must stick to the plan – only use it for the purpose you initially collected it for.

We will only use the information for the purpose we initially collected it for unless additional permissions and safeguards are in effect.

When information is going to be used for a different purpose that isn't directly related to the original one, we may sometimes need to notify the individuals in the same manner as if the information was new or additional information. There are exceptions – for instance, if the information is only being used for research or statistical purposes, and the individuals will not be identifiable in any material published at the end.

Other exceptions may also apply on a case-by-case basis:

For instance where the individual concerned has authorised us to use the information for another purpose, where we took the information originally from a publicly available publication, or where it is necessary to enforce the law or for court proceedings, or to protect public revenue. We can also use information for a purpose other than our original one if we consider it's necessary to protect public health or safety or the life or health of the individual concerned or another individual.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information must only be collected to allow the services proposed to be actioned.	The Fact Find outlines that the information is needed to establish a trust and that the information may also be used for marketing other services provided by the Company.	AML/CFT Act and Trusts Act 2019

IPP 11– Disclosure of Information

Where we hold personal information, we shall not disclose the information to a person or body or agency unless we believe on reasonable grounds, the specified exceptions apply.

What Principle 11 means in practice:

Keep the control – only share information if that's why you got it.

We can disclose information for a particular purpose if that's one of the purposes we originally collected it for, however, if we are being asked to disclose for a different purpose, we will check that we have a good reason and legal authority to do so.

Nobody can use principle 11 to force us to disclose information. Only other statutes or court orders (such as warrants) can make us give information to anybody other than the individual whose information it is. However, principle 11 allows us to disclose information to other organisations if one of the exceptions applies.

The exceptions include:

- where we need to disclose information to an appropriate authority to protect someone (for instance a child who may be at risk)
- where the individual concerned has authorised us to disclose the information to someone else (or we are disclosing it to them)
- where the original source of the information is already publicly available
- where it is for statistical or research purposes and the individual concerned won't be identified
- where disclosing the information is necessary to enforce the law or for court proceedings, or to protect public revenue.

However, as with the use of information (principle 10), these exceptions should be applied on a case-by-case basis and should not be used to justify bulk or regular information sharing.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information should not be shared unless authorised to do so by the client or required by other lawful or legislative purposes.	Section 4 (Confidentially) clause in the client letter of engagement document outlines when information held about them may need to be passed on. Clients sign off that they agree with this. The Fact Find document, page 1 outlines what the information is to be used for. The Company only has two staff members which are both directors of the Company, so there are no unauthorised staff access issues. All information supplied is held within the company and is only passed on where required such as the IRD and the trust's accountant and/or lawyer.	AML/CFT Act and Trusts Act 2019

IPP 12– Disclosing information outside New Zealand

Principle 12 aims to ensure that personal information sent overseas is subject to privacy safeguards that are similar to those in New Zealand.

What Principle 12 means in practice:

We will now be responsible for ensuring that any personal information we disclose to organisations outside New Zealand is adequately protected.

We must be able to demonstrate that we have undertaken necessary due diligence before making a cross-border disclosure.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	Information should only be shared offshore if the recipient is a) subject to the Act b) subject to similar laws in that country c) covered by a binding scheme by Government.	As it relates to New Zealand Family Trust it deals almost exclusively in New Zealand as such information is not required to be sent offshore. There may be circumstances where trustees or beneficiaries reside offshore and information is required to be sent to them. In most cases this will not be personal information. A check on what country the information is to be sent to is to be made to ensure the Privacy legislation and policies of the country are as a minimum up to NZ standards. This will be done by referencing the Privacy study 2019 conducted by comparitech. If the country privacy standards are low then the client is to be contacted to give sign off to have the information sent to the country of concern. A country register is to be maintained outlining each country that information is sent to and what action has taken place. Information is sent to Mexico however this is only sent to the original referrer who supplied the information in the first place.	AML/CFT Act and Trusts Act 2019

IPP 13– Unique identifiers

Principle 13 outlines the importance of not using a client's unique identifier such as an IRD number as the company's identifier.

What will principle 13 mean in practice:

We will not assign any known identifier as our client number. We can assign our own identifier if this is required to carry out our functions and service to the client.

Where we create a client identifier, we must ensure that the client identity has clearly been established.

We will not request any client identifiers from other parties unless it is required to perform our service to the client. i.e. bank account details, IRD number.

Service/Product	Requirements	How actioned	Other regulations
Trust Establishment and administration	To establish a trust in most cases Names, DOB and contact details are needed. ID documents are required in all cases for AML/CFT reason which will show for example passport numbers, driver's license numbers.	Clients are not assigned any unique identifiers from a company perspective, company identification is done via the name of the trust.	AML/CFT Act and Trust Act 2019

Section 3

Breach notifications

What is a Privacy Breach?

A privacy breach is where there has been unauthorised or accidental access to personal information, or disclosure, alteration, loss, or destruction of personal information. It can also include a situation where a business or organisation is stopped from accessing information – either on a temporary basis or permanent basis.

What is a notifiable privacy breach?

If we have a privacy breach that has caused serious harm to someone (or is likely to do so), we will need to notify the Office of the Privacy Commissioner as soon as possible. It is an offence to fail to notify the Privacy Commissioner of a notifiable privacy breach. Failure to notify could incur a fine of up to $10,000.

The Commissioners Office has an online tool on their website, **NotifyUs**, to lodge notifications.

Notifying affected people

If a notifiable privacy breach occurs, we will also notify affected people. This should happen as soon as possible after becoming aware of the privacy breach. Failure to do so may be an interference with person's privacy under the Privacy Act.

There may be valid reasons why we would not notify affected individuals.

What should I include in a notification?

There are key details our organisation must include when notifying the Commissioner's Office and affected people. These details will enable people to protect themselves from harm. The online reporting tool, **NotifyUs**, will guide us through this process.

Why is this important?

When there has been a privacy breach, notifying people lets them take action to protect themselves and their information.

For example, if our online account information is compromised, you can protect yourself by changing your password. If your credit card details are stolen, you can cancel your card. But if you don't know that your privacy has been breached, you can't take any protective action.

What we will do

Where we become aware that any clients or any future staff personal details may have been compromised the PO (Allan Lloyd) will access if the breach is likely to cause serious harm in order to decide whether the breach is a notifiable privacy breach by considering the following:

a) any action taken by us to reduce the risk of harm following the breach

b) whether the personal information is sensitive in nature

c) the nature of the harm that may be caused to affected individuals

d) the person or body that has obtained or may obtain personal information as a result of the breach (if known)

e) whether the personal information is protected by a security measure

f) any other relevant matters.

After analysing the breach and it if is decided that the breach does indeed need reporting then the PO will notify the Commissioner immediately. At the same time the PO will notify the affected person unless section 116 of the Act applies or section 115 (2) where it is not practical to notify all possible clients who have had a breach occur. In this case a public notice should be issued. Section 116 also allows a delay based in certain circumstances.

When reporting to the Commissioner the PO must report the following information:

a) describe the notifiable privacy breach, including—

   i) the number of affected individuals (if known); and

   ii) the identity of any person or body that the agency suspects may be in possession of personal information as a result of the privacy breach (if known); and

b) explain the steps that the Company has taken or intends to take in response to the privacy breach, including whether any affected individual has been or will be contacted; and

c) if the Company is relying on section 115(2) to give public notice of the breach, set out the reasons for relying on that section; and

d) if the Company is relying on an exception, or is delaying notifying an affected individual or giving public notice, under section 116, state the exception relied on and set out the reasons for relying on it or state the reasons why a delay is needed and the expected period of delay; and

e) state the names or give a general description of any other agencies that the Company has contacted about the privacy breach and the reasons for having done so; and

f) give details of a contact person within Company for inquires.

Where we are using section 115 of the Act which is notifying affected persons by a public notice, we must include the following:

a) describe the notifiable privacy breach and state whether the agency has or has not identified any person or body that the agency suspects may be in possession of the affected individual's personal information (but, except as provided below, must not include any particulars that could identify that person or body); and

b) explain the steps taken or intended to be taken by us in response to the privacy breach; and

c) where practicable, set out the steps the affected individual may wish to take to mitigate or avoid potential loss or harm (if any); and

d) confirm that the Commissioner has been notified under section 114; and

e) state that the individual has the right to make a complaint to the Commissioner; and

f) give details of a contact person within the agency for inquiries.

A notification to an affected individual or their representative may identify a person or body that has obtained or may obtain that affected individual's personal information (where the identity is known) if we believe on reasonable grounds that identification is necessary to prevent or lessen a serious threat to the life or health of the affected individual or another individual.

Any notification to an affected individual must not include any particulars about any other affected individuals.

In order to comply with the requirement under sections 114 and 115 that notification must be made as soon as practicable, we may provide the information required by this section incrementally. However, any information that is available at any point in time must be provided as soon as practicable after that point in time.

Compliance notices

The Commissioner may issue us a compliance notice if the following occurs:

a) we are in breach of the Act, including an action listed in section 69(2)(a) of the Act:

b) an action that is to be treated as a breach of an IPP or an interference with the privacy of an individual under another Act:

c) a breach of a code of practice issued under this Act or a code of conduct (or similar) issued under another Act (if a complaint about a breach of the code can be the subject of a complaint under Part 5 of this Act).

If we a served with a compliance notice we must:

a) take steps to comply with the notice, including taking any particular steps specified in the notice.

b) comply with the notice as soon as practicable after receiving it unless it is cancelled or suspended; and

c) if applicable, remedy the breach by the date stated in the notice unless that date is varied or modified.

If a compliance notice is received by the Company the directors of the Company and the PO will arrange a meeting and discuss the contents of the breach and decide if legal counsel is required to be contacted before any remedies are instigated. If legal council is required then the directors to make contact and supply all information supplied by the Commissioner to the legal counsel. No action is to take place until direction from the legal counsel has been obtained.

Once legal counsel has determined what actions the Company should implement, this will be assessed and if agreed will be instigated by the directors in consultation with the PO.

If it is decided not to seek legal counsel the directors and privacy officer to map out the course of action required by the Commissioners directive. These actions are to be instigated by the directors in the time frame stipulated by the Commissioner in consultation with the PO.

Website Privacy Statements

Privacy Policy

At New Zealand Family Trust Services Limited and New Zealand Foreign Trustee Services ("the Companies") we are committed to your privacy. In this Privacy Policy we explain how the Companies collect, store, use and share your personal information.

This Privacy Policy applies to all products and services made available by the Companies including those provided electronically. By using any of the products and services provided by the Companies you are permitting us to collect, store, use and share your personal information in accordance with this Privacy Policy.

What is personal information?

Personal information is information about an identifiable individual. It includes information that could be used to identify you, such as your name and contact details. If the information we collect personally identifies you, or you are reasonably identifiable from it, the information will be considered personal information.

Collection of your personal information

We collect your personal information directly from you unless it is unreasonable or impracticable to do so. When collecting personal information from you, we may collect it in various ways including:

- through your access and use of our website
- by telephone, letter, fax or email
- during conversations between you and our representatives
- by contracting with us or completing relevant forms
- by entering competitions, promotions or requesting information or material from us
- completing surveys, providing feedback or complaining to us.

In some circumstances information may also be collected from third parties where:

- you authorise the collection of information from a third party which may be your representatives such as lawyer, accountant, financial adviser or employer: or
- the information is already publicly available: or
- collection is necessary to enforce the law, or for court proceedings, or to protect public revenue.

If you provide us with personal information about a third party, we collect it on the basis that you have that person's consent for us to collect and handle their personal information in accordance with this privacy policy.

Generally, if we are unable to collect the personal information we require, we may not be able to provide you with the products and services you seek. If the information provided is incorrect or incomplete, this may also prevent, limit or otherwise affect our ability to provide products or services to you.

Terms of use

You can use the site including completing user research tasks without disclosing any personal information.

What purposes do we use your personal information?

We use your personal information to:

- to provide products and services to you and to send communications requested by you;
- to answer enquiries and provide information or advice about existing and new products or services;
- to provide you with access to various areas of our website;
- to assess the performance of the website and to improve the operation of the website;

- for the administrative, marketing (including direct marketing), planning, product or service development, quality control, survey and research purposes of the Companies, related bodies corporate, contractors or service providers;
- to update our records and keep your contact details up to date;
- to process and respond to any complaint made by you; and
- to comply with any law, rule, regulation, lawful and binding determination, decision or direction of a regulator, or in co-operation with any governmental authority of any country (or political sub-division of a country).

Sharing your personal information – purposes

The Companies may use and share your personal information with a range of organisations including:

- authorities such as regulators
- government agencies
- courts or the police
- external dispute resolution schemes
- suppliers and services that may be required to administer our relationship with you such as IT systems administrators, mailing houses, couriers, payment processors, debt collectors.
- professional advisors such as lawyers, accountants, financial advisers, bankers, brokers, and other consultants as it relates to the services provided to you.
- comply with laws and regulations, including any New Zealand or overseas laws, rules, or regulations.
- people of organisations that you expressly give permission to share your personal information with

Storage of your personal information

Your personal information will be stored in a combination of paper files and electronically and are both held internally within New Zealand.

Where your personal information is transferred outside New Zealand we will ensure the intended recipient has provided appropriate safeguards and that requisite rights and remedies in relation to the personal information remain available, or we will obtain your explicit consent for the transfer.

Management of personal information

We take reasonable steps to securely store your personal information to ensure it is protected from unauthorised access, modification and disclosure, and from other types of misuse, interference and loss. This includes electronic and physical security measures and procedures, staff training and use of password protection software.

We will take reasonable steps to destroy or permanently de-identify your personal information when we no longer require it for any purpose for which it was collected. We may retain your personal information for as long as necessary to comply with any applicable law, for legal, insurance and corporate governance purposes, for the prevention of fraud and to resolve disputes. Your personal information may also be retained in our IT system back-up records.

Security of the website

As our website is linked to the internet, and the internet is inherently insecure, we cannot provide any assurance regarding the security of transmission of information you communicate to us online. We also cannot guarantee that the information you supply will not be intercepted while being transmitted over the internet. Accordingly, any personal information or other information which you transmit to us online is transmitted at your own risk.

Cookies

We use cookies and other digital tracking tools (cookies) on the site. A cookie is a small piece of data sent by a website to the browser on your device to help us collect and store information about your use of the website. Some cookies are installed only temporarily while others may remain for a period of time, covering multiple sessions.

We may collect statistical information about your visit to help us improve the site. This information is aggregated and doesn't identify you personally. It includes:

- your IP address
- the search terms you used
- the pages you visited on our site and the links you clicked on
- the date and time you visited the site the referring site (if any) from which you clicked through to this site
- your operating system, for example Windows XP, Mac OS X
- the type of web browser you use, such as Internet Explorer, Chrome or Mozilla Firefox
- other things like your screen resolution and the language setting of your browser.

The Companies and our service providers, use cookies for various purposes, including:

- to measure website traffic and usage patterns and to collect information about your interactions with those services. That information is then used to analyse and improve our services, analyse user behaviour and measure the effectiveness of our marketing initiatives and services;
- to understand your interests and preferences so we can tailor the content to your likely interests along with improving our services and identify suitable offers, products and services from us that we believe may interest you.

How to control cookie settings on your device.

We recommend you enable cookies on your browsers in order to enjoy all the features of our website.

You can block advertising cookies by manually adjusting the cookie settings on your website browser - see the "Help" menu on your browser for details. To learn more about cookies, visit allaboutcookies.org.

Accessing and correcting your personal information

The Companies will do their best to ensure your personal information is accurate. You are responsible for promptly informing us of any change of your personal details (including your name, address, telephone, mobile or facsimile numbers and email address).

You can contact us to request access, or that corrections are made, to the personal information we hold about you. A reasonable fee may be charged to process your request, covering activities such as locating, collating and supplying the information to you.

Under the Privacy Act 2020, in some circumstances we do not have to give you access too or correct your personal information. If that is the case, we will explain why and provide information about how you can complain should you wish to do so.

Resolving your privacy concerns and complaints – your rights

Your satisfaction is our priority so if you have a concern or complaint, please let us know and we'll do our best to resolve it right away. If you're unhappy with our response, you may wish to contact the Privacy Commissioner at privacy.org.nz.

How to contact us

e-mail – info@nzfts.com

Phone – 08000 Trust 08000 87878

P O Box 38-756, Howick, Auckland, 2014,

New Zealand

Changes to this Privacy Policy

From time to time we may make changes to this Privacy Policy, for example to record any changes to the way we handle personal information or the functionality of our services. Notice of any changes will be given at least 14 days in advance, by posting the updated Privacy Policy on our website. Your continued use of our products and services after the end of the notice period will be taken as acceptance of the updated Privacy Policy.

Applicable law

This Privacy Policy is governed by New Zealand law. Your personal information will be collected, used, stored, shared and retained in accordance with this Privacy Policy and New Zealand law. The courts of New Zealand have non-exclusive jurisdiction.

This policy is current as of 12 February 2021

Appendix I – Technology security

Freeparking e-mail

Their system enforces strong passwords for email accounts, and these are used with your email address to authenticate logins for incoming email, and before sending messages.

POP3

Incoming POP3 server host name: mailx.freeparking.co.nz
Secure/Encrypted Connection: Enabled for SSL or SSL/TLS
Port number: 995

IMAP

Incoming IMAP server host name: mailx.freeparking.co.nz
Secure/Encrypted Connection: Enabled for SSL or SSL/TLS
Port number: 993

SMTP

Outgoing SMTP server host name: mailx.freeparking.co.nz
Secure/Encrypted Connection: Enabled for SSL or SSL/TLS
Port number: 465 or 587
Username and password authentication: Enabled and using the same username and password as for the incoming server.