



## PRIVACY POLICY

NEW ZEALAND

VERSION 1

[MAY 2019]

Your Select Home Loan is administered by Bluestone Servicing Limited (FSP181942), Level 21, 151 Queen Street, Auckland, 1010 New Zealand on behalf of the lender, NZGT Custodians (Bluestone) Limited (FSP40011)

## BLUESTONE HOME LOAN PRIVACY POLICY

Nature / purpose of document	This Policy sets out Bluestone's obligations under the Privacy Act 1993 and the Information Privacy Principles. It incorporates our credit reporting policy, that is, it covers additional information on how we handle personal information obtained from credit reporting bodies and certain other consumer credit-related personal information.
Application of policy / distribution	This Policy applies to all Bluestone employees, contractors, consultants, directors and officers. "Bluestone", "we" or "us" means Bluestone Servicing NZ Limited and any related bodies corporate.
Policy owner	Bluestone Legal, Risk & Compliance
Version / last updated	APRIL 2019

## 1. OUR COMMITMENT TO PROTECT CUSTOMER PRIVACY

We understand how important it is to protect our customer's personal information. This document explains how customer's personal information will be treated as they interact with us and with our website.

Our commitment in respect of protecting the customer's privacy is to abide by the Privacy Principles for the protection of personal information, as set out in the Privacy Act 1993 and any other relevant law.

This privacy policy has been drafted to ensure that we manage personal information in an open and transparent way.

This policy will be reviewed annually and we will amend our privacy policy as the need arises, such as to reflect emerging legislative and technological developments, industry practice and market expectations.

## 2. APPLICATION, ACCOUNTABILITY AND COMPLIANCE

This Policy applies to all our employees, contractors, consultants, directors and officers (Bluestone Staff). All Bluestone Staff receive mandatory training relating to this Policy and are expected to comply with this Policy. Bluestone Staff may be required to periodically complete further training related to this Policy. Breaches of this Policy may lead to disciplinary action that may include dismissal.

We will review this Policy periodically. We will amend this Policy as the need arises, such as to reflect emerging legislative and technological developments, industry practice and market expectations.

## 3. PERSONAL INFORMATION

When we refer to personal information, we mean information or an opinion from which a customer's identity is apparent or can reasonably be ascertained. The personal information we hold about a customer may also include credit information.

Credit information is a sub-set of personal information and is information which is used to assess a customer's eligibility to be provided with finance. It may include any finance that a customer has outstanding, a customer's repayment history in respect of those loans, and any defaults. Usually, credit information is exchanged between credit and finance providers and credit reporting agencies (CRAs).

We exchange the customer's credit information with CRAs. We use the credit information that we exchange with the CRAs to assess a customer's creditworthiness, assess the application for finance and manage the finance. If the customer fails to meet his/her payment obligations in relation to any finance that we have provided or arranged, or a customer has committed a serious credit infringement, we may disclose this information to a CRA. We may also complete positive credit reporting with the CRA (see point 5(b) below under the heading Credit information – positive credit

reporting)

A customer has the right to request access to the credit information that we hold about the customer and make a request for us to correct that credit information if needed. We explain how the customer can do this below.

The customer may contact the CRA to advise them that they believe that they may have been a victim of fraud. The customer can contact any of the following CRAs for more information: Equifax New Zealand Information Services and Solutions Limited (<https://www.equifax.co.nz/>) or Dun & Bradstreet (New Zealand) Ltd (<http://dnb.co.nz/>).

#### 4. WHY WE COLLECT YOUR PERSONAL INFORMATION

We may collect (as well as use, hold and disclose) personal information about you for these purposes (Primary Purpose):

- to arrange or provide credit to you (including to action your instructions, to complete your transaction, and to create assessments and ratings of your creditworthiness (such as a credit score));
- to manage that credit (including to assess hardship applications and to collect overdue payments);
- to provide you with industry updates;
- for direct marketing (if you choose to participate) of products and services offered by Bluestone or an organisation Bluestone is affiliated with or represents (including consumer credit insurance);
- to facilitate our operations (including to comply with any legal requirements);
- to manage our relationship with you (including to invoice you and to deal with any complaints or enquiries); and
- for statistical and security purposes.

We may also collect (and use) your personal information for the purpose of establishing a customer loyalty program.

If you do not want to provide us with your personal information, we may not be able to arrange or provide credit to you or provide other services. We also may not be able to verify your identity or protect against fraud.

#### *Cookies*

A "cookie" is a small text file placed on your computer by a webpage server that may later be retrieved by webpage servers. We use cookies on our website to provide you with a better website experience.

Our use of cookies does not allow us to collect personally identifiable information about you, but is or may be used (for example) to determine if you have previously visited our website or other websites, to personalise your web browsing experience, to

track and report on website usage and performance, and for statistical and security purposes.

You can configure your browser to refuse cookies or delete existing cookies from your hard drive. Rejecting cookies may have the effect of limiting access to or functionality of parts of our website.

## 5. INFORMATION PRIVACY PRINCIPLES

We have set out the heading of each of the Privacy Principles below and we set out the steps we take to ensure that Bluestone complies with the principles:

**(a)** Principle 1 - *Purpose of collection of personal information*

We will only collect personal information where it is necessary for the Primary Purposes and other purposes as set out above that are connected with a functions or activities of Bluestone.

**(b)** Principle 2 - *Source of personal information*

With the exception of credit reports or unless it is unreasonable or impracticable to do so, we will only collect your personal information directly from you during the course of our business relationship.

We will only do so by lawful and fair means. If you contact us (for example, through our website), we may keep a record of that contact and information you provided during that contact.

Occasionally, we may collect personal information about you from other sources including public sources, referring parties and information brokers. For example, we may collect such information from a CRA or referring party in the course of assisting you in securing financial arrangements, from public registers when checking the security you are offering, from your employer to confirm details of your employment, or from your landlord to confirm details of your residence and rental payment. Some of the personal information we collect from or about you is collected to meet our obligations under the *Credit Contracts and Consumer Finance Act 2003* and the AML/CTF Act.

*Credit information – positive credit reporting*

In addition to the above, we may collect the following kinds of credit information and exchange this information with CRAs and other entities, this is sometimes called “positive credit reporting”.

- (i)** Identification information.
- (ii)** Consumer credit liability information being information about your existing finance which includes the name of the credit provider, the type of finance, the day the finance is entered into, the terms and conditions of

the finance, the maximum amount of finance available, and the day on which the finance was terminated.

- (iii) Repayment history information (RHI), which is information about whether you meet your repayments on time. See more under “repayment history information” below.
- (iv) A record of a lender asking a CRA for information in relation to a credit application, including the type and amount of credit applied for.
- (v) Publicly available records relating to your activities in New Zealand and your credit worthiness.
- (vi) Personal insolvency information, which is a record relating to your bankruptcy or your entry into a debt agreement or personal insolvency agreement.
- (vii) Information on serious credit infringement, which is a record of when a lender reasonably believes that there has been a fraud relating to your consumer credit or that you have avoided paying your consumer credit payments and the credit provider cannot find you.
- (viii) Information about the type of finance that you are applying for or have applied for.
- (ix) Default and payment information, including new arrangement information, where a lender gave a CRA default information about you and your consumer credit contract is varied or replaced, a statement about this.
- (x) Court proceedings information.

We exchange this credit information for the purposes of assessing your application for finance and managing that finance.

When we obtain credit information from a CRA about you, we may also seek publicly available information and information about any serious credit infringement (for example, fraud) that you may have committed.

We may disclose your credit information to overseas entities that provide support functions to us - see IPP10 and IPP11 on “Limits on use of personal information” and “Limits on disclosure of personal information”.

(c) Principle 3 - *Collection of information from subject*

At or before the time of collecting your personal information and unless we consider that Privacy Principle (3) sub-clause (4) applies, we will take reasonable steps to ensure you are aware of:

- (i) the fact that we are collecting information,
- (ii) the purposes for which the information is collected,
- (iii) the organisations that are the intended recipients of the information,
- (iv) the name and address of the agencies holding the information,
- (v) if we are collecting information due to an authorisation at law, then we

will state the name of the law and whether the information is mandatory or voluntary,

- (vi) the consequences (if any) if all or any part of the requested information is not provided; and
- (vii) the customer's right to access and correct the personal information collected.

For example, we do so in the privacy consent form we ask you to sign, via our website privacy statement which is publicly and freely available and in this Policy.

(d) Principle 4 - *Manner of collection of personal information*

We will not collect personal information by unlawful means, or by means that, in the circumstances of the case, are unfair, or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

(e) Principle 5 - *Storage and security of personal information*

We may store your personal information in paper and electronic form. We may use cloud storage to store the personal information we hold about you.

We have a range of technical, administrative and other security safeguards to protect your personal information from interference, misuse, loss, unauthorised access, modification or disclosure, including:

- (i) any paper records are accessible to Bluestone Staff only on a "as needed" basis;
- (ii) we have a "clean desk" policy for all Bluestone Staff and it requires, for example, that all paper records to be held within an office that is locked at night;
- (iii) control of access to our building;
- (iv) our electronic databases are password access only with virus protection software and firewalls installed;
- (v) our physical storage is protected by security measures such as alarm systems and security patrol; and
- (vi) all Bluestone Staff receive mandatory training relating to this Policy.

If we store personal information physically or electronically with third party data storage providers, we will use contractual arrangements to ensure those providers take appropriate measures to protect that information and restrict the uses of that information.

(f) Principle 6 - *Access to personal information*

You may request access to the personal information we hold about you. We will need to verify your identity before allowing access.

When you request access to your personal information, we will conduct a search on our database. This search will also indicate if there are any paper records that contain personal information.

We will give access in the manner you have requested if it is reasonable to do so. We may charge you a fee for our cost of retrieving and supplying the information. If we do, the fee will not be excessive and will not apply to the making of the request.



We will respond to your request within a reasonable period but in not more than 20 working days unless we write to you (following the requirements in s40 of the Privacy Act) and advise that we need to extend the time for compliance due to the nature of the request and the volume of information held.

Depending on the type of request that you make, we may respond to your request immediately, otherwise we usually respond to you within seven days of receiving your request. We may need to contact other entities to properly investigate your request.

We may deny you access to your personal information if:

- (i) the information disclosure would affect the security, defence or international relations of New Zealand or the listed territories set out in s27 of the Privacy Act 1993.
- (ii) the withholding of the information is reasonably necessary, after taking into consideration the public interest considerations that weigh in the favour of disclosure, to protect information where the making available of the information—
  - would disclose a trade secret; or
  - would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information.
- (iii) the disclosure of the information would involve the unwarranted disclosure of the affairs of another individual or of a deceased individual; or
- (iv) the disclosure of the information or of information identifying the person who supplied it, being evaluative material, would breach an express or implied promise—
  - which was made to the person who supplied the information; and
  - which was to the effect that the information or the identity of the person who supplied it or both would be held in confidence; or
- (v) the disclosure of the information would breach legal professional privilege; or
- (vi) the disclosure of the information would constitute contempt of court or of the House of Representatives; or
- (vii) the request is frivolous or vexatious, or the information requested is trivial.
- (viii) if the information requested is not readily retrievable; or the information requested does not exist or cannot be found; or the information requested is not held by the agency and the person dealing with the request has no grounds for believing that the information is either—
  - held by another agency; or
  - connected more closely with the functions or activities of another agency.

The term “evaluative material” means evaluative or opinion material compiled solely:

Your Select Home Loan is administered by Bluestone Servicing Limited (FSP181942), Level 5, 125 Queen Street, Auckland, 1010 New Zealand on behalf of the lender, NZGT Custodians (Bluestone) Limited (FSP40011)

a) for the purpose of determining the suitability, eligibility, or qualifications of the individual to whom the material relates—

- for employment or for appointment to office; or
- for promotion in employment or office or for continuance in employment or office; or
- for removal from employment or office; or
- for the awarding of contracts, awards, scholarships, honours, or other benefits; or

(b) for the purpose of determining whether any contract, award, scholarship, honour, or benefit should be continued, modified, or cancelled; or

(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property.

**(g)** *Principle 7 - Correction of personal information*

You may request us to correct the personal information we hold about you. We will respond to your request within a reasonable period and within 20 working days. We will take reasonable steps to correct your personal information to ensure that, having regard to a purpose for which it is held, it is accurate, if either:

- (i)** we are satisfied that it needs to be corrected; or
- (ii)** you request that your personal information be corrected.

We may need to consult with other entities as part of our investigation. Where reasonable, and after our investigation, we will provide you with details about whether we have corrected the personal information within 30 days.

If there is disagreement as to whether the information is accurate, at your request we will take reasonable steps to associate with the information a statement claiming that the information is not accurate.

We will not charge you for making the request, for correcting the information or for associating a statement with the information.

If we correct personal information about you that it has previously disclosed to another entity, we will take reasonable steps to notify the other entity of the correction.

If we decide not to give make a correction, we will provide reasons for the refusal and information on how you can complain about the refusal.

*Credit information - specific rules*

The most efficient way for you to make a correction request is to send it to the organisation that made the mistake.

If we are able to correct the information, we will let you know within five business days of deciding to do this. We will also let the relevant third parties know as well as any others you tell us about. If there are any instances where we cannot do this, then we will let you know in writing.

If we are unable to correct your information, we will explain why in writing within five business days of making this decision. If you have any concerns, you can access our external dispute resolution scheme or make a complaint to the Office of the Privacy Commissioner (OPC).

If we agree to correct your information, we will do so within 20 working days from when you asked us, or a longer period that's been agreed by you.

If we cannot make corrections within 20 working days or the agreed time frame, we will explain why and let you know when we expect to resolve the matter, ask you to agree in writing to give us more time, and let you know you can complain to our external dispute resolution scheme or the OPC. See more under "complaints" below.

**(h)** Principle 8 - *Accuracy, etc, of personal information to be checked before use*

We will take reasonable steps to ensure that your personal information is accurate, up-to-date, complete, relevant and not misleading (collectively referred to as "accurate" below). We request (for example, in the privacy consent form we ask you to sign, via our website privacy statement which is publicly and freely available and in this Policy) that you contact us at any time to update, change or correct your personal information if you think the information we have is not accurate. See IPP13 on "correction of personal information". We will generally rely on you to ensure the information we hold about you is accurate, up-to-date or complete.

In terms of uses and disclosures, we will take reasonable steps to ensure that your personal information is accurate, having regard to the purpose of that use or disclosure.

**(i)** Principle 9 - *Agency not to keep personal information for longer than necessary*

We will not keep your personal information for longer than is necessary for the Primary Purposes and other purposes, however, we are likely to need to retain your information for a long time.

We will usually destroy personal information that is held in paper and electronic form seven years after our relationship with the individual ends (unless that information we have to retain it by or under New Zealand law or a court/tribunal order). We will do this by shredding paper copies and deleting electronic records containing personal information about the individual or permanently de-identifying the individuals within those records.

Sometimes it is impossible or impractical to completely isolate the information then completely remove all traces of the information, and we may store the information for future use, such as to help resolve disputes between us or assess future applications by you. The same security safeguards will be in place to protect the information.

(j) Principle 10 - *Limits on use of personal information* & Principle 11 – *Limits on disclosure of personal information*

*How we use and disclose personal information*

We are committed to treating your personal information as confidential. Other than for the Primary Purpose, we will only use or disclose your personal information if:

- i. we have your consent;
- ii. the use or disclosure is required or authorised by or under a New Zealand law or a court/tribunal order;
- iii. we reasonably believe that the use or disclosure is necessary to lessen or prevent a serious threat to someone's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain your consent;
- iv. we need to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to our functions or activities;
- v. the use or disclosure is to an enforcement body for certain enforcement related activities (and we will make a written note of this as required by IPP6.5); or
- vi. the use or disclosure is reasonably necessary to assist an IPP entity to locate a missing person, for certain activities relating to a legal or equitable claim, or for a confidential alternative dispute resolution process.

If we choose to disclose to a CRA consumer credit liability information in relation to consumer credit provided to you, we will, once that credit is terminated or otherwise ceases to be in force, disclose this to the CRA within 45 days of that date.

*With whom do we exchange personal information*

We may use, disclose and exchange personal information with the following types of entities (Exchange Entities), some of which may be located overseas

- i. Credit providers.
- ii. Any person who proposes to guarantee or has guaranteed repayment of any credit provided by you or any joint borrowers.
- iii. CRAs.

Your Select Home Loan is administered by Bluestone Servicing Limited (FSP181942), Level 5, 125 Queen Street, Auckland, 1010 New Zealand on behalf of the lender, NZGT Custodians (Bluestone) Limited (FSP40011)

- iv. Finance or mortgage brokers, mortgage originators, mortgage managers, and persons who assist us to provide our products to you.
- v. Financial consultants, accountants, lawyers, valuers and other advisers.
- vi. Any industry body, tribunal, court or otherwise in connection with any complaint regarding the approval or management of your loan (for example, if a complaint is lodged about any mortgage broker or lender who dealt with your loan).
- vii. Businesses assisting us with funding for loans (for example, a credit enhancer, funder or rating agency).
- viii. Trade insurers, mortgage insurers and title insurers.
- ix. Any person where we are required by law to do so (for example, pursuant to subpoena or to a government agency such as tax authorities in Australia and overseas).
- x. Any of our associates, agent, related entities (in Australia and overseas) or contractors (for example, statement printing houses or mail houses).
- xi. Your referees (for example, your employer) to verify information you have provided.
- xii. Any person considering acquiring an interest in our business or assets.
- xiii. Any organisation providing verification (including on-line verification) of your identity.

Before we disclose any of your personal information to another entity, we will take all reasonable steps to satisfy ourselves that the entity has a commitment to protecting your personal information at least equal to our commitment or you have consented to us making the disclosure.

#### *Verification of your identity using information held by a CRA*

We may verify your identity using information held by a CRA. To do this, we may disclose personal information such as your name, date of birth, driver licence number, or passport details and address to the CRA to obtain an assessment of whether that personal information matches information held by the CRA. The CRA may give us a report on that assessment and to do so may use personal information about you and other individuals in their files. Alternative means of verifying your identity are available on request.

When we collect a driver licence number from you for disclosure to the credit reporter, we will: (a) make clear to you that the provision of the driver licence number is voluntary; (b) collect the driver licence card number from you and disclose this to the credit reporter; and (c) where the driver licence number and driver licence card number are collected from you in person, take reasonable steps to ensure that you are the individual shown on the driver licence.

We exchange your credit information with CRAs. We use the credit information that we exchange with the CRAs to assess your creditworthiness, assess your application for finance and managing your finance. If you fail to meet your

payment obligations in relation to any finance that we have provided or arranged, or you have committed a serious credit infringement, we may disclose this information to a CRA.

You have the right to request access to the credit information that we hold about you and make a request for us to correct that credit information if needed. This is explained below.

You may contact the CRA to advise them that you believe that you may have been a victim of fraud. You can contact any of the following CRAs for more information:

Equifax New Zealand Information  
Services and Solutions Limited (371729)  
PO Box 912012, Victoria St West,  
Auckland 1142  
[www.mycreditfile.co.nz](http://www.mycreditfile.co.nz)

Dun & Bradstreet (New Zealand) Ltd  
PO Box 9589, Newmarket, Auckland  
1031  
<http://dnb.co.nz>

#### Direct marketing

We may use or disclose your personal information (other than sensitive information) for the Primary Purpose, including for direct marketing, but only if you have not made a request not to participate in direct marketing (such as by contacting us to opt out). If the direct marketing is by email or SMS, you may also use the unsubscribe function. We will not charge you for making a request to opt out, and we will give effect to your request within a reasonable period.

Other than by email and SMS, we may also conduct direct marketing activities via telephone, mail or any other electronic means. We may also market to you through third party channels (such as social networking sites).

We may use or disclose your personal information (other than sensitive information) for direct marketing under circumstances where you would reasonably expect us to use or disclose the personal information for direct marketing.

We will obtain your consent before using or disclosing sensitive information for the purpose of direct marketing.

We do not disclose your personal information to any third party for the purpose of allowing them to market their products or services to you.

#### Cross-border disclosures

We may exchange personal information with the Exchange Entities, some of which may be located overseas. This includes Australia, the United Kingdom, Ireland and the United States. While these entities will often be subject to confidentiality or privacy obligations, they may not always follow the particular requirements of New Zealand privacy laws.

We may store your information in cloud or other types of networked or electronic storage. As electronic or networked storage can be accessed from various countries via an internet connection, it is not always practicable to know in which country your information may be held. If your information is stored in this way, disclosures may occur in countries other than those listed.

Overseas organisations may be required to disclose information we share with them under a foreign law. We are not responsible for such disclosure.

We will not share any of your credit information with a CRA unless it has a business operation in New Zealand. We are not likely to share credit eligibility information (that is, credit information we obtain about you from a CRA or that we derive from that information) with organisations unless they have business operations in New Zealand. (See more under “credit eligibility information” below.) We are likely to share other credit information about you with organisations outside New Zealand, as per the countries listed above.

**(k)** Principle 12 - *Unique identifiers*

We do not adopt a government related identifier (such as your tax file number or driver’s licence number) as a means of identifying you.

We do not use or disclose your government related identifier unless:

- i. it is reasonably necessary for us to verify your identity for the purposes of our activities or functions;
- ii. we need to fulfil an obligation to the relevant government body or we are prescribed by regulations to do so;
- iii. we reasonably believe that the use or disclosure is necessary to lessen or prevent a serious threat to someone’s life, health or safety, or to public health or safety;
- iv. we need to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to our functions or activities;
- v. the use or disclosure is required or authorised by or under an New Zealand law or a court/tribunal order; or (xxiii) the use or disclosure is to an enforcement body for certain enforcement related activities.

## 6. ENQUIRIES AND COMPLAINTS

Your Select Home Loan is administered by Bluestone Servicing Limited (FSP181942), Level 5, 125 Queen Street, Auckland, 1010 New Zealand on behalf of the lender, NZGT Custodians (Bluestone) Limited (FSP40011)

### *Enquiries*

If you have any queries or would like further information about this Policy, please contact us by telephoning 0800 668 333 or by writing to us at [complaints@select.bluestone.net.nz](mailto:complaints@select.bluestone.net.nz).

If you would like further advice regarding your privacy rights, you can contact the OPC by visiting website <https://www.privacy.org.nz>

### *Complaints*

If you believe that our privacy standards do not meet the privacy principles or you have a complaint about our handling of your personal information, please contact us by telephoning 0800 668 333 or by writing to us at [complaints@select.bluestone.net.nz](mailto:complaints@select.bluestone.net.nz). We will endeavour to investigate and advise you of the outcome of your complaint as soon as possible.

We have in place Dispute Resolution (DR) procedures, which we will follow in handling your complaint. We will provide our customers with a copy of our DR procedures free of charge if one is requested.

If you are not satisfied with the outcome, you may complain to the OPC or to an external dispute resolution scheme we are a member of called Financial Services Complaints Limited. The contact details of Financial Services Complaints Limited are:

Phone: 0800 347 257      Website: [www.fscl.org.nz](http://www.fscl.org.nz)      Email: [complaints@fscl.org.nz](mailto:complaints@fscl.org.nz)  
Business address: Level 4, 101 Lambton Quay, Wellington, 6011  
Postal: PO 5967, Wellington 6145

## 7. PRIVACY BREACHES

We recognise that the improper use or disclosure of personal information may pose a risk of financial, reputational or other harm to the affected person.

There are potentially significant costs to Bluestone if we do not meet our obligations to protect or maintain personal information (Breaches). Breaches (such as sending a communication that contains personal information to the wrong recipient) may result in fines, damage to our reputation and loss of trust from our customers.

### *Breach prevention*

Security is a basic element of information privacy. We are committed to preventing Breaches and we have a range of technical, administrative and other



security safeguards in place to protect your personal information from interference, misuse, loss, unauthorised access, modification or disclosure (which we have outlined under IPP5 on “*Storage and Security of Personal Information*” above).

### *Dealing with Breaches*

We will deal with Breaches in an appropriate and timely manner.

There may be internal and external actions that need to be taken. In taking any action, we will be guided by these steps as suggested by the OPC on responding to a Breach (whether it is actual or suspected):

1. Containment: Your preliminary assessment - what has happened, and is there anything you can do to retrieve or secure the personal information
2. Evaluation: Consider the risk associated with the breach – what potential harm could result in this case, and is there anything you can do to minimise this harm?
3. Notification: Should affected parties be made aware of the breach, and, if so, how will you notify them
4. Prevention: What lessons can be learned from this experience to prevent future breaches or to better respond if there is another breach?

See also: <https://www.privacy.org.nz/data-breaches/data-safety-toolkit/>

For example, a Bluestone Staff who has identified a Breach or any suspicious activity will, as soon as practicable, escalate to the Compliance Manager and Legal for assessment and evaluation. The Compliance Manager and/or Legal (as appropriate) will, first, determine whether any notification to the affected individual or regulator is necessary, then conduct a risk assessment to identify measures that could be taken to reduce the likelihood of a future breach.