BLUESTONE GROUP PTY LTD
ABN: 20 091 201 357

PRIVACY POLICY
INCORPORATING CREDIT REPORTING POLICY

VERSION 4
[October 2018]
OWNER: BLUESTONE LEGAL, RISK & COMPLIANCE

Bluestone Privacy Policy	
Nature / purpose of document	This Policy sets out Bluestone's obligations under the Privacy Act and the Australian 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 Group Pty Limited (ACN 091 201 357), Bluestone Servicing Pty Limited (ACN 122 698 328) and any related bodies corporate.
Policy owner	Bluestone Legal, Risk & Compliance
Version / last updated	October 2018

1. Introduction

We understand how important it is to protect our customers' personal information. It is important to us that you are confident that any personal information we collect from you or received by us will be treated with appropriate respect. This document sets out our privacy commitment to our customers (referred to as "you").

Any personal information we collect about you will only be used for the purposes indicated in this privacy policy (Policy) or as allowed under the law. Our commitment in respect of personal information is to abide by the *Australian Privacy Principles* (APPs) for the protection of personal information, as set out in the *Privacy Act 1988 (Cth)* (Privacy Act) and any other relevant law. The APPs replace the *National Privacy Principles* for organisations from 12 March 2014. The APPs regulate the way in which organisations like us can collect, use, keep secure and disclose personal information.

This Policy is also known as our "APP privacy policy" as referred to in APP1.3. It incorporates our credit reporting policy that sets out our approach to the collection, handling and disclosure of your consumer credit-related information, for example, information about your credit applications and your credit reporting information that we obtain from credit reporting bodies (CRBs). When we refer to our privacy policy in general or "this Policy" in this document, we are also referring to the incorporated credit reporting policy unless the context provides or requires otherwise.

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. Definition of personal information

When we refer to *personal information*, we mean information from which your identity is apparent. This information may include information or an opinion about you, from which your identity can reasonably be ascertained.

Credit information is a sub-set of personal information and is information that is used to assess your eligibility to be provided with finance. It may include any finance that you have outstanding, your repayment history in respect of those loans, and any defaults. Usually, credit information is exchanged between credit and finance providers and CRBs. When we refer to credit *reporting* information, we mean credit information or information derived by a CRB. When we refer to credit *eligibility* information, we mean credit information we obtain about you from a CRB

or that we derive from that information. These terms may be confusing but they are as defined by the Privacy Act. See more on "credit eligibility information" below.

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. Privacy principles

We abide to the 13 APPs set out in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)* (which amends the Privacy Act) in the following manner.

(a) APP1: Open and transparent management of personal information

Our ongoing practices and policies are documented in this Policy to enable us to manage personal information in an open and transparent way. This Policy contains specified information, including the kinds of personal information we collect, how you may complain about a breach of the APPs, and whether we are likely to disclose information to overseas recipients. We will provide our customers with a copy of this Policy free of charge at any time if one is requested.

(b) APP2: Anonymity and pseudonymity

If it is ever practicable to do so, we will provide you with the option not to identify yourself or to use a pseudonym (a fake name) when dealing with us. However, given the nature of our services, other laws that regulate banking and financial services (including *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* (AML/CTF Act)) and our contractual obligations to third parties, these options are mostly not available to you.

(c) APP3: Collection of solicited personal information

Personal information in general

As explained above, we collect personal information from you for the Primary Purpose.

Examples of personal information we collect for the Primary Purpose includes the following.

(i) Full name, and any alias or previous names.
(ii) Date of birth.
(iii) Current and previous addresses, and length of time at these addresses.
(iv) Account details.
(v) Occupation and job title, and length of time at your current job.
(vi) Contact information.
(vii) Transaction information about your matter.
(viii) Ages and number of your dependants and cohabitants.
(ix) Interests in consumer and commercial credit products or services and related products and services.
(x) Income, expenses and similar financial information.
(xi) Any information we may need to identify you.

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 CRB 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 *National Consumer Credit Protection Act 2009 (Cth)* and the AML/CTF Act.

Credit information – specific rules

In additional to the above, we may collect the following kinds of credit information and exchange this information with CRBs and other entities. (This is sometimes called "positive credit reporting".) See APP8 on "cross-border disclosures" for more on these "Exchange Entities".

(i) Identification information.
(ii) Consumer credit liability information being information about your existing finance which includes the name of the credit provider, whether the credit provider holds an Australian Credit Licence, 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 CRB 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 Australia 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 CRB 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.

This credit information may be held by us in electronic form on our secure servers and may also be held in paper form. We may use cloud storage to store the credit information we hold about you.

When we obtain credit information from a CRB 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 APP6 on "use and disclosure of personal information" and APP8 on "cross-border disclosures".

Sensitive information

Sensitive information is any information about your racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information.

We may seek and collect sensitive information about you but only if that sensitive information relates directly to our ability to arrange or provide credit to you or manage the credit provided to you.

(b) APP4: Dealing with unsolicited personal information

Sometimes people share information (including sensitive information) with us we have not sought out. This could be through using our website, making a general enquiry, requesting us to resolve a dispute or requesting us to assess a hardship application. We may also receive unsolicited personal information about you (including sensitive information) by mistake. If we receive such information about you, we will determine whether we would have been permitted to collect the information under APP3 and for the Primary Purpose. If yes, then all the following items (that is, APP5 to APP13) will apply to that information. If no and the information is not contained in a Commonwealth record, then we will destroy or de-identify it as soon as practicable, but only if it is lawful and reasonable to do so.

Often, it is not possible for us to neatly unbundle this information then destroy or de-identify only certain sections or parts of it, and we may need to store this information for future use, such as to help resolve disputes between us or assess future applications by you. We have many security safeguards in place to protect the information from interference, misuse, loss, unauthorised access, modification or disclosure. See more under APP11 on "security of personal information" below.

(c) APP5: Notification of the collection of personal information

At or before the time of collecting your personal information, we will take reasonable steps to ensure you are aware of the purposes for which the information is collected and the organisations to which information of that kind are usually disclosed. 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.

We will also take reasonable steps to ensure you are aware of the access, correction and complaints processes. 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) APP6: Use and 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:

(xii) we have your consent;
(xiii) the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order;
(xiv) 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;
(xv) 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;
(xvi) 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 APP6.5); or
(xvii) the use or disclosure is reasonably necessary to assist an APP 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 chooses to disclose to a CRB 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 CRB 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 - see APP8 on "cross-border disclosures".

(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) CRBs.
(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 CRB

We may verify your identity using information held by a CRB. To do this, we may disclose personal information such as your name, date of birth and address to the CRB to obtain an assessment of whether that personal information matches information held by the CRB. The CRB 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. If we are unable to verify our identity using information held by a CRB, we will provide you with a notice to this effect and give you the opportunity to contact the CRB to update your information held by them.

"Notifiable matters"

The law requires us to advise you of "notifiable matters" in relation to how we may use your credit information. You may

request to have these notifiable matters (and this Policy) provided to you in an alternative form, such as a soft copy.

We exchange your credit information with CRBs. We use the credit information that we exchange with the CRBs 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 CRB.

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.

Sometimes, your credit information will be used by CRBs for "pre-screening" credit offers on the request of other credit providers. You can contact the CRB at any time to request that your credit information is not used in this way.

You may contact the CRB to advise them that you believe that you may have been a victim of fraud. For 21 days after the CRB receives your notification, the CRB must not use or disclose that credit information. You can contact any of the following CRBs for more information:

- Dun & Bradstreet (Australia) Pty Ltd (www.dnb.com.au or 1300 734 806)
- Experian (www.experian.com.au or 1300 783 684)
- Veda Advantage Ltd (www.veda.com.au)

(b) APP7: 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 reasonable 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.

(c) APP8: Cross-border disclosures

We may exchange personal information with the Exchange Entities, some of which may be located overseas. This includes New Zealand, the Philippines, 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 Australian 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 CRB unless it has a business operation in Australia. We are not likely to share credit eligibility information (that is, credit information we obtain about you from a CRB or that we derive from that information) with organisations unless they have business operations in Australia. (See more under "credit eligibility information" below.) We are likely to share other credit information about you with organisations outside Australia. A list of countries in which those overseas organisations are located is set out above.

(d) APP9: Adoption, use or disclosure of government related 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:

(xviii) it is reasonably necessary for us to verify your identity for the purposes of our activities or functions;
(xix) we need to fulfil an obligation to the relevant government body or we are prescribed by regulations to do so;
(xx) 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;
(xxi) 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;

(xxii) the use or disclosure is required or authorised by or under an Australian law or a court/tribunal order; or

(xxiii) the use or disclosure is to an enforcement body for certain enforcement related activities.

(b) APP10: Quality of personal information

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 APP13 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.

(c) APP11: Security of personal information

We may store your personal information in paper and electronic form. 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 are 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.

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 is contained in a Commonwealth record, or we have to retain it by or under an

Australian 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.

(d) APP12: Access to personal information

Personal information in general

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. 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) we reasonably believe that the denial is necessary to lessen or prevent a serious threat to someone's life, health or safety, or to public health or safety;
(ii) giving access would have an unreasonable impact on the privacy of other individuals;
(iii) the request for access is frivolous or vexatious;
(iv) the information relates to existing or anticipated legal proceedings between us, and the information would not be accessible by the process of discovery in those proceedings;
(v) giving access would reveal our intentions in relation to negotiations with you in such a way as to prejudice those negotiations;
(vi) giving access would be unlawful;
(vii) denying access is required or authorised by or under an Australian law or a court/tribunal order;
(viii) we have reason to suspect that there is or may be unlawful activity or serious misconduct that relates to

our functions or activities, and giving access would be likely to prejudice us in taking of appropriate action;

(ix) giving access would be likely to prejudice enforcement related activities by an enforcement body; or

(x) giving access would reveal evaluative information we have generated in connection with a commercially sensitive decision making process.

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

If we refuse to give access or we cannot give access in the manner you have requested, access may be given through the use of a mutually agreed intermediary.

Credit information – specific rules

In additional to the above, regarding a request to access credit information, we will:

(i) respond substantively within 30 days of the request for access;

(ii) present the credit information clearly and provide reasonable explanations and summaries of the information; and

(iii) advise you to access your credit information from a CRB for the most up to date information.

(b) APP13: Correction of personal information

Personal information in general

You may request us to correct the personal information we hold about you. We will respond to your request within a reasonable period. 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:

(xi) we are satisfied that it needs to be corrected; or

(xii) 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 APP entity, we will take reasonable steps to notify the other APP 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 Australian Information Commissioner (OAIC).

If we agree to correct your information, we will do so within 30 days from when you asked us, or a longer period that's been agreed by you.

If we cannot make corrections within 30 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 OAIC. See more under "complaints" below.

---

2. Specific issues

(a) Repayment history information

Background

Repayment history information, or RHI, is information about whether you have made or missed a consumer credit payment.

As part of the reforms to the Privacy Act, new kinds of credit-related personal information can be collected about you. This includes whether you have made or missed a consumer credit payment. This new type of information is called "repayment history information".

RHI explained

RHI is information about whether you have met your consumer credit payment obligations. Consumer credit is credit that is

intended to be used primarily for personal, family or household purposes.

RHI includes information about whether you have made a payment on time or whether you have missed a payment. The grace period we allow for an overdue payment is five days. If you only pay part of the amount owing, you are taken to have missed a payment.

RHI includes the day on which a payment is due, and if you made a payment after that day, the date on which you paid. Therefore, RHI can include both positive and negative information about your credit history.

RHI does not include the amount of any missed payment — only the fact that you have made or missed a payment.

RHI can include information about any consumer credit payments that you make, or fail to make, to a credit provider that holds an Australian Credit Licence. This means that RHI will usually reflect made or missed payments on a loan or credit card.

Collection of RHI

We may collect RHI about you in relation to payments falling due on or after 1 December 2012. We can disclose this information to CRBs from 12 March 2014.

Use and disclose of RHI

We may use or disclose RHI about you to help service you, such as to determine your eligibility to be provided with credit.

We do not disclose RHI about that credit more frequently than once each month.

(b) Credit eligibility information

What is credit eligibility information

Credit *eligibility* information is credit information we obtain about you from a CRB or that we derive from that information. (This is different from credit *reporting* information, which means credit information or information derived by a CRB.)

The law places limits on use and disclosure of credit eligibility information by "credit providers" (as defined by the Privacy Act, which includes Bluestone).

Limits on the use of credit eligibility information

We may use the credit eligibility information we hold about you:

(i) for consumer credit related purposes; or

(ii) where we believe you have committed a serious credit infringement and the credit eligibility information is used in connection with the infringement.

If we obtained your credit eligibility information for consumer credit related purposes, then it can be used for:

(i) securitisation related purposes; or
(ii) internal management purposes related to the provision of the consumer credit.

If the credit eligibility information was:

(i) obtained for commercial credit purposes, then it may only be used for that purpose;
(ii) obtained for assessing an application for commercial credit, then it may also be used for internal management purposes directly related to the provision or management of that commercial credit;
(iii) obtained for guarantee purposes, then it may also be used for internal management purposes in addition to the credit guarantee purpose;
(iv) disclosed to us because we already held consumer credit liability information, then it may also be used for assisting you to avoid defaulting on your obligation in relation to consumer credit provided by us; or
(v) disclosed for securitisation related purposes, then it may only be used for that purpose.

We can disclose your credit eligibility information to:

(i) you;
(ii) to a related body corporate;
(iii) to a person for processing an application or a person who manages credit;
(iv) to another credit provider with an Australian link if we reasonably believe that you have committed a serious credit infringement; or
(v) an external dispute resolution scheme if we are a member of that scheme.

Limits on the disclosure of credit eligibility information

In addition to be above, we are permitted to disclose credit eligibility information about you under the following circumstances.

Regarding other credit providers: We can disclose your credit eligibility information to other credit providers:

(i) if the disclosure is for a particular purpose, the recipient has and Australian link, and you have expressly consented to the disclosure (this usually means if you have signed our privacy consent form, unless the credit eligibility information is for the purpose of assessing an application for consumer credit that is not yet in writing);

(ii) we are acting as an agent of another credit provider in assessing of an application for credit or managing the credit and we make the disclosure as agent;

(iii) if we are involved in a securitisation arrangement and the disclosure is reasonably necessary for the purchasing, funding, managing, or processing of an application for credit by means of a securitisation arrangement or undertaking credit enhancement in relation to the credit;

(iv) if we and they other credit provider have provided mortgage credit in relation to the same secured real property and have an Australian link, you are at least 60 days overdue in making a payment, and the credit eligibility information is disclosed for the purpose of either credit provider deciding what action to take in relation to the overdue payment.

Regarding guarantees: We can disclose your credit eligibility information if we have provided credit to you or you have applied for credit, the disclosure is for considering whether to act as a guarantor or to offer property as security for the credit, the guarantor has an *Australian link*, and you expressly consent to the disclosure (this usually means if you have signed our consent form).

Regarding mortgage insurers: We can disclose credit eligibility information if the disclosure is to a mortgage insurer with an Australian link for lenders mortgage insurance purposes or any purpose arising under a contract for lenders mortgage insurance.

Regarding debt collectors: We can disclose credit eligibility information if the debt collector carries on a business that involves the collection of debts on behalf of others, disclosure is for the primary purpose of collecting overdue payments to either consumer credit or commercial credit, and the disclosure is of identification information, court proceedings information, or personal solvency information.

Regarding other recipients: We can disclose credit eligibility information if the disclosure is to any of these recipients that have an Australian link - a government agency, small business or other organisation subject to the APPs, or a professional legal or financial adviser of the entity. The recipient may use the credit eligibility information for exercising the rights associated with, or considering whether to, accept an assignment of debt, accept a debt owed to us as security for credit provided to us, or purchase an interest in us or a related body corporate.

Where there is no Australian link

If we disclose credit eligibility information to an entity with no Australian link, we will take reasonable steps to ensure the overseas entity does not use or disclose the credit eligibility information other than in accordance with Australian legislation and ensure the overseas entity does not breach the APPs.

(b) Information to be given if an application for credit is refused

If your application for consumer credit has been refused by us on the basis of your or your guarantor's information held by a CRB, the law requires us to, within a reasonable time after refusing the application, to give written notice of the refusal, state that the refusal was wholly or partially based on that information held by the CRB, and if the information is about you (as opposed to the guarantor), then state the name and contact details of the CRB.

If information from a CRB obtained in the previous 90 days forms part of the basis for the refusal, the law also requires us to provide written notice within 10 business days of the date of the refusal decision. We will keep a record of the notice. The notice will explain your right to access (and how to access) your credit reporting information free of charge during the 90 days following the notice, that it is important that you be proactive in checking the accuracy of the credit reporting information the CRB holds about you, state we rely upon information from a number of sources to make our decision (including information provide by you such as the security of your employment), and how you can access and correct the credit eligibility information we hold (as detailed in this Policy).

(c) Information to be given prior to listing default information with a CRB

The law requires is to give you notice if we intend to list default information with a CRB. Firstly, we will give you a "section 6Q notice" regarding default information, informing you of the overdue payment and requesting that you pay the overdue amount. Default information relates to information about an overdue payment of over $150 in relation to consumer credit if you are 60 days overdue in making the payment.

30 days after providing the section 6Q notice, we will then give you a "section 21D notice". It will state our intention to disclose, after 14 days of the notice, the overdue amount specified in the notice (taking into consideration any payments made) to the CRB. We cannot make this disclosure if 3 months has lapsed after the section 21D notice.

If an overdue payment is made, we will take reasonable steps to disclose the payment information to the CBR within 3 business days.

We will not disclose an overdue payment in relation to consumer credit to a CRB as default information if you have made a hardship request and we are processing that request, or 14 days has lapsed after we have notified you of the decision.

2. Enquiries and complaints

Enquiries

If you have any queries or would like further information about this Policy, please contact us by telephoning (02) 8115 5000 or 13 BLUE or by writing to us at PO Box 1136, QVB Post Shop, NSW, 1230.

If you would like further advice regarding your privacy rights, you can contact the OAIC by email at enquiries@oaic.gov.au or by phone on 1300 363 992.

Complaints

If you believe that our privacy standards do not meet the level set by the 13 APPs or have a complaint about our handling of your personal information, please contact us by telephoning (02) 8115 5000 or 13 BLUE or by writing to us at PO Box 1136, QVB Post Shop, NSW, 1230. We will endeavour to investigate and advise you of the outcome of your complaint as soon as possible.

We have in place Internal Dispute Resolution (IDR) procedures. We will follow this procedure in handling your complaint. We will provide our customers with a copy of our IDR procedures free of charge if one is requested.

If you are not satisfied with the outcome, you may lodge a complaint with the Australian Financial Complaints Authority (AFCA). AFCA provides fair and independent financial services complaint resolution that is free to consumers.

Website:	www.afca.org.au
Email:	info@afca.org.au
Phone:	1800 931 678 (free call)
Mail:	Australian Financial Complaints Authority GPO Box 3, Melbourne VIC 3001

If you are still not satisfied, you can complain to the OAIC using the details provided above.

3. 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 APP11 on "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 OAIC on responding to a Breach (whether it is actual or suspected):

Step 1: Contain the Breach and do a preliminary assessment
Step 2: Evaluate the risks associated with the Breach
Step 3: Notification
Step 4: Prevent future Breaches

A copy of the OAIC's "Data Breach Notification - a guide to handling personal information security breaches" can be accessed at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches.

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.