EDINBURGH REALTY PRIVACY POLICY

VERSION 1 – DECEMBER 2020

INTRODUCTION

This policy explains how and when Edinburgh Realty collects personal information, what we do with it and your right to see or change it. Edinburgh Realty complies with the New Zealand Privacy Act 2020 (the **Act**) when dealing with personal information. Personal information is information about an identifiable individual (a natural person).

This policy sets out how we will collect, use, disclose and protect your personal information.

This policy does not limit or exclude any of your rights under the Act. If you wish to seek further information on the Act, see www.privacy.org.nz.

CHANGES TO THIS POLICY

We may change this policy by uploading a revised policy onto the website. The change will apply from the date that we upload the revised policy.

This policy was last updated on 1st December 2020.

WHO DO WE COLLECT YOUR PERSONAL INFORMATION FROM

We collect personal information about you from:

- you, when you provide that personal information to us, including via the website and any related service, through any registration or subscription process, through any contact with us (e.g. telephone call or email), or when you buy or use our services and products
- third parties where you have authorised this or the information is publicly available.

If possible, we will collect personal information from you directly.

HOW WE USE YOUR PERSONAL INFORMATION

We may use your personal information:

- *to verify your identity as per our requirements under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009*
- *to provide services and products to you*
- *to market our services and products to you, including contacting you electronically (e.g. by text or email)*
- *to undertake credit checks of you (if necessary)*
- *to bill you and to collect money that you owe us, including authorising and processing credit card transactions*
- *to respond to communications from you, including a complaint*
- *to conduct research and statistical analysis (on an anonymised basis)*
- *to protect and/or enforce our legal rights and interests, including defending any claim*
- *for any other purpose authorised by you or the Act.*

DISCLOSING YOUR PERSONAL INFORMATION

We may disclose your personal information to:

- *any business that supports our services and products, including any person that hosts or maintains any underlying IT system or data centre that we use to provide the website or other services and products*
- *a credit reference agency for the purpose of credit checking you*
- *other third parties*
- *a person who can require us to supply your personal information (e.g. a regulatory authority)*
- *any other person authorised by the Act or another law (e.g. a law enforcement agency)*
- *any other person authorised by you.*

A business that supports our services and products may be located outside New Zealand. This may mean your personal information is held and processed outside New Zealand.

PROTECTING YOUR PERSONAL INFORMATION

We will take reasonable steps to keep your personal information safe from loss, unauthorised activity, or other misuse.

- **Passwords and Electronic Email Subscriptions**
    - All work computers are password protected.
    - Cellphones that are owned and controlled by Edinburgh are all password protected.
    - Any personal electronic subscriptions or logins to websites and other accounts should be setup with a personal email address. Edinburgh email is only to be used for work related communications.
    - Work computers should be locked when leaving desks for breaks/lunch.
    - Managers will hold password information for staff devices in a secure file that is only accessible to certain staff.
- **AML**
    - We currently use AML Hub as a third-party app to securely collect information for the purposes of AML identity verification. This is our recommended and preferred method of gathering this data and all agents are encouraged to utilise it if possible.
    - Any photos or documents collected directly must be loaded to the app as soon as practicable and the original image deleted off the device. Regular reviews of device storage should be done to ensure nothing is retained.
    - Where we have been requested to forward on ID's (eg to a solicitor), this request must be received by each individual concerned in writing and uploaded into the AML Hub. The administrator can upload the written request for you.
- **Personnel Files**
    - Physical files are kept in a locked filing cabinet in the General Managers office, which is locked daily.
    - Digital copies of information are kept in a file on the server that is only accessible by management.
    - Information on former employees are securely destroyed 6 months after they leave.
    - Non-current information that is required to be stored for 7 years is kept securely in a locked filing room that is only accessible by management.
- **Salespeople**
    - Contractors are treated similarly to employees under the act. Therefore Edinburgh may be held responsible for the actions of a contractor if there is a breach under the Privacy Act. The contractor may also be held personally liable for any breach. If the contractor is acting outside of the express or implied terms of the agencies authority however, the agency may not be liable.
    - Client databases are managed through a secure online portal.
- **Open Home Registers, Sale and Purchase Agreements, Listing Forms etc.**
    - Handwritten documents (open home registers etc) contain a disclosure statement stating the reason we are collecting the information. Information collected on these registers include name, address, phone number and email and will only be used for marketing purposes or work expressly related to real estate.
    - Sale and Purchase agreements are stored in a secure locked management office. These will be reviewed and destroyed after the required 7 years.

    - No personal contact details are to be shared or forwarded to anyone else without the consent of the individual who own those details.
- **Various Software**
    - We utilise RealNZ which is password protected for individual users.
    - Palace is our online property management portal. Information held through this includes information on our tenants, landlords and suppliers. This system is password protected.
    - We also use online portals Preno and Staah which collects guest information and stores it securely.
- **Administrators**
    - Administrators are required to have a clear desk at the end of each day and any documents need to be put in a drawer etc. No documents to be left on the desk and all personal information should be disposed of in the secure document destruction bin.
- **Destruction of Personal Information**
    - It is company policy that ALL documents that contain personal information are destroyed only using our professional document destruction company. There are two locked wheelie bins stored at either end of the building for this purpose.
- **Privacy Breach Ban**
    - A privacy breach is any unauthorised or accidental access to, disclosure, alteration, loss or destruction of personal information, or an action that prevents the holder from accessing the information.
    - Any privacy breaches must be reported to the Privacy Officer immediately – despite the seriousness. The Privacy Officer and Managing Director will then determine if the breach is of such significance that it needs to be reported to the Privacy Commissioner. Any minor breaches will be thoroughly reviewed by the Privacy Officer to determine the cause and how to prevent a future breach.
    - Not all breaches will need to be reported to the Privacy Commissioner, only those that cause serious harm. Determining if a breach has or might cause serious harm will be a case-by-case assessment, taking into account things like disclosure of very sensitive information or to a large number of recipients, and the nature of the harm that might result. Failing to inform the Privacy Commissioner about a notifiable privacy breach is an offence.
- **Annual Privacy Review**

The Privacy Officer will review the policies and procedures on an annual basis.

- **IT Partners**

Datacom are our software providers and review our various software regularly to ensure they are satisfied with their privacy policies and software architecture.

ACCESSING AND CORRECTING YOUR PERSONAL INFORMATION

Subject to certain grounds for refusal set out in the Act, you have the right to access your readily retrievable personal information that we hold and to request a correction to your personal information. Before you exercise this right, we will need evidence to confirm that you are the individual to whom the personal information relates.

In respect of a request for correction, if we think the correction is reasonable and we are reasonably able to change the personal information, we will make the correction. If we do not make the correction, we will take reasonable steps to note on the personal information that you requested the correction.

If you want to exercise either of the above rights, email us at dunedin@edinburgh.co.nz. Your email should provide evidence of who you are and set out the details of your request (e.g. the personal information, or the correction, that you are requesting).

We may charge you our reasonable costs of providing to you copies of your personal information or correcting that information.