



## PRIVACY POLICY

### Policy Snapshot

We are committed to protecting your<sup>1</sup> privacy in compliance with our legislative obligations. We will only collect, use, handle and disclose personal data as allowed by, and in compliance with, the privacy legislation applicable to us.

### Your privacy is important to us

QIC Limited and its subsidiaries (together 'QIC', 'we' or 'our') are committed to protecting your privacy, in compliance with all local privacy laws covering our operations in Australia, the UK and the US.

We are committed to being open about how we use personal data and this Policy sets out how we handle your information.

By providing personal data to us, you consent to our collection, use and disclosure of your personal data in accordance with this Policy and any other arrangements that apply between us. We may change our Policy from time to time by publishing changes to it on our website. We encourage you to check our website periodically to ensure that you are aware of our current Policy.

### Collection of information

We limit our collection of personal data<sup>2</sup> to those details we identify as reasonably necessary for the lawful purposes of our business.

Being a wholesale funds manager, we do not collect or hold personal data in relation to individual members of funds who invest with us. Personal data will only be collected by lawful and fair means from the individual concerned or their authorised representative. The collection of 'sensitive data'<sup>3</sup> will only be in accordance with the law.

QIC will advise of the use of and seek your consent prior to processing your personal data. It is at your discretion whether you provide QIC with this information, however, failure to supply relevant information may mean we are unable to maintain or provide products or services to you.

---

<sup>1</sup> Please note the Privacy Act 1988 (Cth) does not apply to the handling of personal data directly related to a current or former employment relationship with QIC or to employee records held by QIC. However, where required by law in other jurisdictions, this Privacy Policy also extends to employee related data.

<sup>2</sup> Personal data includes Personal Information under The Privacy Act 1988 (Cth) and includes any information:

(a) Relating to an identified or identifiable natural person;

(b) An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

<sup>3</sup> 'Sensitive data' is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. As a general rule, the only type of sensitive data we hold is in relation to an individual's professional or trade association membership.

We will inform you at or before the time of collection (or as soon as possible afterwards) of the purposes for collection, to whom your data might be disclosed and any other relevant details that will help you to ensure we are protecting your privacy. In some instances, we may direct you to this Policy for this information.

We take reasonable steps to keep personal data as accurate, complete, and up-to-date as is necessary for the purposes we have identified.

## Handling of information

We only collect and use data for the purpose of providing our products or services, including sending you information, or undertaking our business. In relation to our Global Real Estate business, we collect and use personal data for purposes in connection with the management, administration, operation and promotion of our retail and commercial properties. Examples of who we usually collect data from, types of data, purposes for collection and method of collection are contained in a Table in Appendix 1.

## Do Not Track Signals

Some web browsers incorporate a “Do Not Track” (DNT) or similar feature that signals to digital devices that a visitor does not want to have his/her online activity tracked. Because not all web browsers offer DNT options and DNT signals are not yet uniform, we and many other website operators do not respond to DNT signals.

## Links

Our website may contain links to websites operated by third parties. Those links are provided for convenience and may not remain current or be maintained. Unless expressly stated otherwise, we are not responsible for the privacy practices of, or any content on, or security of those linked websites, and have no control over or rights in those linked websites. The privacy policies that apply to those other websites may differ substantially from this Policy, so we encourage individuals to read them before using those websites.

## Disclosure of information

At QIC, personal data is strictly confidential. We will only disclose personal data in accordance with the law. We may disclose your personal data:

- to other companies within the QIC group;
- to our insurers and insurance brokers;
- to our commercial and joint-venture partners;
- to third parties who perform services for us;
- to law enforcement or government agencies, including where necessary to meet our statutory obligations;
- where it is required or authorised by law;
- where we use it for the purposes for which it was collected; or
- where you have consented to the disclosure of your personal data.

You may provide QIC with data outside of your home country, or we may use and disclose your personal data overseas, including to recipients located in countries where we have an overseas office as listed here. By consenting and providing your personal data to QIC, you agree to this processing.

## Overseas disclosure of personal data

We may from time to time disclose your personal data to third party suppliers and service providers located overseas (including providers for the operation of our websites and/or our business or in connection with providing our products and services to you). We will not send your personal data outside Australia unless it is authorised by law and we can be satisfied that the recipient of the personal data has adequate data protection arrangements in place. Recipients outside the jurisdictions set out in this policy may also be subject to a foreign law that could compel the disclosure of personal data to a third party, such as an overseas authority.

Any data sharing will be in compliance with the local privacy laws and governed by our strict standards and policies, and where appropriate, confidentiality and other agreements to ensure your information is secure and treated with the utmost care and respect.

## Storage of information

We protect personal data with appropriate safeguards and security measures and restrict access to those who have a legitimate business purpose and reason for accessing it. Personal data is only retained for as long as it is necessary for the identified purposes or as required by law.

QIC takes steps to protect the security of the personal data we hold from both internal and external threats through the following safeguards:

Security safeguard	Details
Physical Security	The security features of QIC’s major datacentres and access to infrastructure, including servers and databases are regularly audited, including physical building structure, electronic locks, alarms, video recording devices, UPS, power generators, redundant air-conditioning and environmental / infrastructure monitoring. Access is strictly limited to authorised administration staff only. Strict processes are in place for the removal of physical, network, remote and application access as required by Human Resources management processes.
Staff awareness and education	As part of our data governance processes, QIC conducts a cyber-security education and awareness program. The program consists of computer based learning, classroom seminars, information bulletins and physical media. It provides enterprise wide general awareness training, help desk training, application software security training and live phishing scenario testing.
Robust monitoring and oversight	Regular security assessments are performed on all critical IT assets, systems and third parties.
System security	Network controls such as firewalls, Intrusion Prevention, Anti-Virus, Web Application Firewall, Advanced Threat Detection, Data Loss Prevention, system hardening, Wireless Access Controllers and secure network design provide protection for all devices on the QIC network. QIC’s password policy

	uses expiry, strength and reuse rules. Our remote access functionality operates with RSA two-factor authentication.
Destroying data when no longer required	Where practical, we keep information only for as long as required (for example, to meet legal requirement our internal needs).

## Information access and correction

At QIC, decisions and actions may be taken or made on the basis of personal data in our possession and we take reasonable steps to keep personal data as accurate, complete, and up-to-date as is necessary.

Should you, or your authorised representative, want to exercise your right to access, modify, correct, or restrict your personal data, we may ask you to put such a request in writing. We may require identification to ensure the person requesting access is entitled to such access. If you, or your representative, is denied access to your information, we shall provide reasons for the denial.

If we are reasonably satisfied our records need correcting, we will make the correction as soon as possible. If we do not agree our records need correcting, we will inform you of the reason(s) and you may require us to keep a statement on our records that you believe the information is inaccurate, incomplete, misleading, irrelevant or not up-to-date.

In the event you would like QIC to delete, stop processing, or withdraw consent for, your personal data to the extent you are entitled to under applicable law, you can make such a request in writing.

If you are a registered member of one of our Shopping Centre membership programs, you may be able to access and update the information on your member profile in the applicable section of the Shopping Centre website. You may also access and update your personal data as part of your use of any of our Shopping Centre ‘opt-in’ services, such as Wi-Fi services and frictionless parking services<sup>4</sup>.

## Opting Out of Communications

If you receive direct marketing communications from us, you may easily request not to receive such communications from us by:

- following the instructions on the communication to opt-out or unsubscribe from further communications;
- if you are a member of one of our Shopping Centre membership programs, by logging into the member area on the Shopping Centre website and ticking the opt-out option;
- contacting your usual QIC contact; and
- contacting our Privacy Compliance Officer or Data Protection Officer.

## Resolving enquiries or complaints

If you have any questions, concerns or complaints about the treatment of your personal data, the first step is to discuss the issue with your usual QIC contact. Any privacy related breaches will be managed in accordance with our Breaches and Incidents Policy.

If your concerns have not been resolved to your satisfaction, please contact our Privacy Compliance Officer on +61 7 3360 3922 or by email at [privacy@qic.com](mailto:privacy@qic.com). In the US, please contact our Chief Compliance Officer

---

<sup>4</sup> Neither QIC’s website nor its Shopping Centre websites are directed to individuals under the age of 13, and we do not knowingly attempt to solicit or receive information from children under 13 years of age.

on +61 421 899 605 or by email at [privacy@qic.com](mailto:privacy@qic.com). In the EU or UK please contact our Data Protection Officer on +61 7 3020 7446 or by email at [privacy@qic.com](mailto:privacy@qic.com) or our UK Data Protection Representative on +44 20 7092 8220 or by email at [privacy@qic.com](mailto:privacy@qic.com). We may ask you to put your query in writing.

If after contacting our Privacy Compliance Officer your concerns remain unresolved, you may contact the Office of the Australian Information Commissioner on 1300 363 992 or by email on [enquiries@oaic.gov.au](mailto:enquiries@oaic.gov.au). You can also visit their website at [www.oaic.gov.au](http://www.oaic.gov.au).

In the U.K., you may contact the Information Commissioner's Office on 0303 123 1113, or you can also visit their website at [www.ico.gov.uk](http://www.ico.gov.uk). For individuals based in Europe, please contact any other competent supervisory authority of an EU Member State.

## Further Information

QIC Limited 130 539 123

This document is subject to the [QIC Disclaimer and website access terms and conditions](#).

## Version History Update

**Non-material changes approved by the Chief Risk Officer (11 May 2017) are as follows:**

- a) Added contact details for the DPO and UK Data Protection Representative
- b) Included existing IT security controls
- c) Updates in line with changes in Australian and EU data protection legislation
- d) Updates in line with US specific legislation such as the California Online Privacy Protection Act of 2003 and the Children's Online Privacy Protection Act of 1998 (COPPA)



## Appendix 1

Person	Types of information	Identified purposes	Method of collection
Key individuals employed by our investment clients or their representatives	Business and personal contact details, family information (such as name of spouse/partner, and details of children), social preferences (information which enables us to tailor events and entertainment), special dietary information	Client relationship management, business development, seminars and other client events, and for the conduct of daily business operations including the identification of clients as required by law or regulation	Verbally or by email, directly from the individual or personal assistant / secretary where permitted by law
Potential employee candidates	Employment history, experience, qualifications, contact details, and checks as to criminal history, personal insolvency and regulatory sanction	Assessment for suitability for a current or future position	Resumes received from applicants in response to positions advertised, or unsolicited resumes, or completion of a criminal history / insolvency check form (or by way of a response received from an external agency verifying the details provided on the form)
Industry-related contacts and other individuals interested in QIC or the funds management industry	Contact details (including job title and name of their organisation)	Distribution of newsletters and other publications to provide regular information about the views and operations of QIC	Directly from the individual, either verbally or via a form for updating details
Individuals who supply (or are employed by organisations that supply) goods or services to QIC – this includes those who facilitate our investment transactions	Contact details and bank account details (where financial transactions are undertaken)	In relation to the supply of the goods and services and to facilitate the credit and payment arrangements	From the individual directly, usually verbally or from transaction documentation
Individuals in respect of who we are obliged by law to conduct AML/CTF checks	Copies of identification documents	To enable QIC to comply with our AML/CTF obligations	Directly from the individual, either verbally or via a form for collecting details

Person	Types of information	Identified purposes	Method of collection
In relation to retail and commercial properties held as assets of QIC investment funds associated with our Global Real Estate business ( <i>GRE Properties</i> ):			
Individual tenants, licensees and guarantors (and key individuals associated with corporate tenants, licensees and guarantors) of leases and licences of GRE Properties (including potential tenants, licensees and guarantors and associated key individuals)	Information collected may include: Contact details, date of birth, ABN, financial and trading information, business experience, insurance details, and copies of identification documents	Leasing and licensing negotiations, decisions (including assessing applications) and documentation, managing tenancy design and delivery process, operational tenancy and Shopping Centre communications, relationship management, issuing invoices and notices, sale of premises, providing access to marketing retailer portal and monitoring performance and value of GRE Properties	Leasing and licensing applications and documentation; communications with tenants, licensees, guarantors and solicitors
Customers (or other individual visitors) of retail GRE Properties (Shopping Centre)	Information collected may include: Contact details (including name, address, phone number, gender, email address, interest, date of birth), shopping preferences, interests, photographic and video images	Direct marketing (e.g., promotional activities, distribution of e-newsletters, advertising (including third party advertising), and other publications and communications and mobile push notifications). Administration of events and promotional activities at the Shopping Centres (including competitions and promotions) Administration of our Shopping Centre gift card program. Providing services to customers at Shopping Centres (for example, mobility aid hire services, lost and found services and other services to benefit customers) Photographic and video images are used for security purposes or for promotional activities	Directly from the individual, either verbally or via a form for collecting details. For images, from video surveillance cameras when customers visit our Shopping Centre or when using cameras for promotional activities

Person	Types of information	Identified purposes	Method of collection
<p>Individuals who use websites associated with our Shopping Centres or our Global Real Estate business, who use free Wi-Fi services provided at our Shopping Centres, who interact with us through social media pages associated with our Shopping Centres or who download and use our Shopping Centre smartphone applications</p>	<p>Information collected may include:            Contact details (including name, address, phone number, gender, email address, date of birth), shopping preferences, interests, social media IDs, likes and areas of interest, IP address or the fully qualified domain name from which the individual accessed our website, the date and time an individual accesses our website, the web browser that is being used by the individual to access our website and the pages accessed and the URL of any webpage from which the individual accessed our website</p>	<p>Direct marketing (e.g., promotional activities, distribution of e-newsletters, advertising (including third party advertising) and other publications and communications and mobile push notifications)            Administration of events and promotional activities at the Shopping Centres (including competitions and promotions)            Administration of our Shopping Centre gift card program            Customising and improving our website and e-newsletter content</p>	<p>Directly from the individual when they sign up for membership of a Shopping Centre membership program, register for an event, sign-up to receive communications regarding opportunities or offers associated with one or more Shopping Centres or participate in a competition or promotion or access a free Wi-Fi service at a Shopping Centre            We use cookies to track usage of our website</p>
<p>Individuals who supply goods or services or carry out works in respect of GRE Properties (or are employed or engaged by organisations that do so)</p>	<p>Information collected may include:            Contact details, ABN, financial information, insurance details, business experience</p>	<p>Tendering, contract negotiations, decisions and documentation in relation to the supply of the goods and services or the works, operational communications, and to issue and process invoices</p>	<p>From the organisation or from the individual directly (either verbally or through quotes, correspondence, tender forms or contract documentation), through contractor induction and compliance processes</p>