



Employee Privacy Policy

This privacy policy was last updated on 4 June 2026.

Introduction

PwC is strongly committed to protecting personal information. This privacy policy describes why and how we collect and use personal information and provides information about individuals' rights. It applies to personal information provided to us, both by individuals themselves or by others. We may use personal information provided to us for any of the purposes described in this privacy policy or as otherwise stated at the point of collection.

This privacy policy applies to PricewaterhouseCoopers (NZBN 9429044819965), PwC Legal (NZBN 9429042425953), PricewaterhouseCoopers Consulting (New Zealand) LP (NZBN 9429043294114) and PwC Foundation (NZBN 9429050409716), of Level 26 PwC Tower, 15 Customs Street West, Auckland 1010, New Zealand, and any entity owned or controlled by these entities' operations in New Zealand (together "PwC", "we", or "our"). This policy explains how PwC handles personal information relating to its **employees, independent contractors and partners** and complies with the requirements of the Privacy Act 2020 ("Privacy Act"). If you have any further questions in relation to this policy, please contact our Privacy Officer at nz_privacy_officer@pwc.com. Our privacy policy for personal information collected from clients, suppliers, and other individuals is available at <https://www.pwc.co.nz/privacy.html>. Applicants who submit an online job application can view the privacy policy relevant to the job application process at [ATS Privacy Statement](#).

Personal information or personal data is information about an identifiable living person. When "you" or "your" are used in this statement, we are referring to the relevant individual who is the subject of the personal information.

Processing is how we sometimes refer to the handling, collecting, protecting or storing of your personal information.

When collecting and using personal information, our policy is to be transparent about why and how we do that.

1. Collection of personal information

PwC collects, holds and processes personal information from job applicants, employees, independent contractors and partners for necessary business, employment and compliance purposes.

The types of personal information we collect, hold and process include:

- Personal information collected from job applicants when they apply for a job with us and individual contractors when performing a role for us (in some instances this may include sensitive information such as health information if related to the role being applied for or being performed).
- Basic information about you, such as name, gender, date of birth, home address, telephone number, email address
- Government and other identifiers (for instance IRD number, passport number)
- Employment-related details, such as job title, salary, benefits and organisational role
- Internal identifiers and system log-in details (such as GUID, staff ID and passwords to access PwC IT facilities)
- Photographs, images, recordings and reproductions of your voice, likeness or image (e.g. on ID cards and security systems, profiles and through the use of CCTV)
- Personal information collected from our employees during the course of carrying out our duties and activities as an employer (in some instances this may include sensitive information such as health information if related to the employee's role). This may include administrative and performance related information (e.g. job applications, background screening and references, qualifications, training, skills, timesheet records, expense claim data, payroll and benefits information, holiday and absence records, performance records, grievance and disciplinary records)
- Health, disability and wellbeing information, such as sick leave and medical certificates, fitness for work assessments, workplace injuries and ACC information, reasonable accommodations, mental health and wellbeing support, vaccination or infectious disease information, if relevant.
- Compliance related data (e.g. fit and proper records, investments and other financial interests, details of business and family relationships).
- General user and technical information, such as internet protocol addresses, browser type, internet service provider details, authentication, user logs, device data and similar technical information, when employees use PwC websites, applications or related systems. We also collect certain metadata derived from automated scanning of emails, chat messages, printing records, downloads and web page access and, from time to time, we may access the content of suspicious emails, documents or other files sent or received by you to determine whether they represent a security threat or a threat to client confidentiality. Similarly, we collect premise access information (e.g. use of staff ID cards to access, leave or move between restricted areas of PwC's premises), and phone records. Collection of this information may be event-based, continuous, targeted, random or triggered by alerts, but only where lawful, reasonable and necessary for a legitimate business, employment, security, legal, regulatory, health and safety, confidentiality, client-protection or compliance purpose.

In limited contexts, we collect sensitive personal information. Sensitive personal information includes information about an individual's race or ethnic origin; political opinions or political affiliations; religious or philosophical beliefs; trade union membership; physical or mental health; genetic data; biometric data that uniquely identifies someone; sexual life or sexual orientation; and criminal records. For instance, we may request that you provide your ethnicity, for the purposes of analysing the diversity of the talent we attract. We also collect health information, where necessary to support and manage your working relationship with us. If you choose to provide sensitive personal information about yourself to us for any reason, the act of doing so constitutes your explicit consent, (where such consent is necessary), for us to collect and use that information as necessary in the ways described in this privacy policy or as described at the point you choose to disclose this information.

We collect most information directly from individuals when we deal with them. The personal information we collect may be provided in forms filled out by individuals, face to face meetings, email messages, telephone conversations, when you use our websites or our social media, or by third parties. If you contact us, we may keep a record of that contact. Because of the nature of our business, it is generally impracticable for us to deal with individuals on an anonymous basis or through the use of a pseudonym, although sometimes this is possible (for example, when seeking staff feedback generally).

We may collect personal information about you from third parties, including referees, former employers, recruitment agencies, background screening providers, government agencies, professional bodies, clients, PwC network firms or benefits providers. Where required by the Privacy Act, we will take reasonable steps to tell you that we have collected that information, the purpose of collection, the intended recipients, the agencies collecting and holding it, whether collection is authorised or required by law, and your rights to access and correct it. This policy may be supplemented by more specific notices at or around the time of collection where required, particularly where the indirect collection is sensitive, unusual, investigation-related, or not reasonably expected.

In some instances, we collect from you certain information relating to other individuals, for example details of:

- A person to contact in case of emergency
- Your dependents / spouse in relation to the provision of employee benefits as applicable
- Information entered into PwC's Checkpoint system, compliance questionnaires and other regulatory returns regarding spouses, co-habitees and dependents (e.g. names, addresses and financial interests)

It is your responsibility to ensure that any such individual has been informed that his/her personal information will be shared with us for the applicable purposes. It is also your responsibility to ensure that you share this Privacy Policy with them. You will be asked to confirm that you have done so.

2. Our legal grounds for processing personal information

We rely on one or more of the following conditions to justify processing your personal information:

- Our legitimate interest in the lawful operation of our business
- Our legitimate interests in maintaining the security of our and our client's data and in ensuring the quality of our services
- Our legitimate interest in developing and improving our business, and the employee experience
- To satisfy any requirement of law, regulation or professional body of which we are a member
- To perform our obligations under a contractual relationship with employees; or
- Where no other processing condition is available, if you have agreed to us processing your personal information for the relevant purpose.

In some instances, if you do not provide us with specific information, we will be unable to administer your employment. For example, if you do not provide your IRD number, KiwiSaver information, or Right to Work information we may be unable to pay you or meet our legal obligations.

3. Why we process personal information

We use your Personal information in connection with your role with us. The primary purposes for which we collect, hold and process personal information are:

- For recruitment purposes, including analysing the diversity of the talent we attract
- For performing the contract between you and us, including each of us exercising our respective rights under it
- To plan, manage and run our business (including providing professional services to our clients, resourcing, engagement planning, execution and review, marketing and business development)
- Managing our relationship with you, including the provision of remuneration and benefits, undertaking appraisals, performance evaluation and management, operating learning, development and employee experience initiatives
- Monitoring your compliance with relevant policies including the PwC Network's regulations, applicable laws and professional rules, and employment laws and obligations
- Providing health, safety and wellbeing at work, including keeping our offices open safely and contacting emergency contacts as required
- Enabling your participation in PwC equality and diversity initiatives (including membership to PwC networks)
- For undertaking insights analysis about our workforce, in an aggregate form. This may include gender, ethnicity, health information or other sensitive information.
- Providing references, either for internal transfers or in connection with transfers to other PwC network firms or third party employers
- Security, quality and risk management activities: we have security measures in place to protect our and our client's information (including personal information), which involves detecting, investigating and resolving security threats. This may include:
 - Automated scans to identify harmful emails or targeted monitoring in response to an alert;
 - Monitoring the services provided to clients for risk and quality purposes, which may involve processing personal information stored on the relevant client file.
 - Carrying out conflict and risk searches to ensure there are no issues that would prevent us from working with a particular client (such as sanctions, criminal convictions (including in respect of company directors), conduct or other reputation issues);
- Investigating or establishing whether you have committed an unlawful act, or been involved in any dishonesty, malpractice or improper conduct. In this context, investigations include employment investigations, bullying, harassment and conduct matters, conflicts of interest and independence investigations, regulatory or client related investigations, litigations or threatened litigation.
- Managing our business in connection with an actual or potential sale, transfer, disposal, merger or restructure of a part of our business or as part of an acquisition or merger with another business
- Complying with any requirements of law, regulation or a professional body of which we are a member
- Other purposes related to our business, where lawful and reasonably connected with the purposes described in this policy.

If you choose not to provide us with personal information which we have requested from you, we may be unable to fulfil any of the above purposes, including responding to your requests or processing your application for employment.

If we collect, hold or use personal information in ways other than as stated in this policy, we will ensure we do so pursuant to the requirements of the Privacy Act.

4. Disclosure of personal information

PwC does not disclose your personal information unless:

- Disclosure is permitted by this policy
- We believe it is necessary for maintaining, or is related to, your role at PwC
- To protect the rights, property or personal safety of any member of the public or a customer of PwC or the interests of PwC
- Some or all of the assets or operations of PwC are or may be transferred to another party as part of the sale of some or all of PwC's business
- You give your consent
- Such disclosure is otherwise required or permitted by law, regulation, rule or professional standard.

We may also disclose personal information under the following circumstances:

- To our professional advisers, for example, law firms, as necessary to establish, exercise or defend our legal rights and obtain advice in connection with the running of our business;
- To other PwC network firms, as necessary in connection with your role including the provision of shared IT and security services
- To clients, potential clients and business contacts, where appropriate in connection with client engagements. For instance, experience information / CVs of our personnel may be shared.
- When explicitly requested by you;
- When required to facilitate training, conferences or events hosted by a third party; or
- To third party contractors, subcontractors, and/or their subsidiaries and affiliates (for example independent contractors and consultants, travel service providers, mail houses, off-site security storage providers, information technology providers, event managers, credit managers, debt collecting agencies, providers of identity management, website hosting and management, data analysis, data backup, security and cloud storage services).

We may also share non-personal, de-identified and aggregated information for research or promotional purposes. Except as set out in this policy, we do not sell to or trade personal information with third parties.

Please note, in accordance with the above, sometimes individuals and organisations outside of PwC will have access to personal information held by PwC and may collect or use it from or on behalf of PwC. Some of these third party providers may use their own third party subcontractors that have access to personal information (subprocessors). It is our policy to use only service providers and third party providers that are bound to maintain appropriate levels of security and confidentiality, to process personal information only as instructed by PwC and in accordance with our privacy guidelines and not to keep, use or disclose personal information we provide to them for any unauthorised purposes. We also require the flow of those same obligations down to their sub-processors. We will only share personal information with others when we are legally permitted to do so.

5. Retention

We retain personal information for as long as is necessary for the purpose for which it was collected and in accordance with our Retention Policies. Personal information may be held for longer periods where extended retention periods are required by law or regulation and as necessary in order to defend our legal rights.

6. Transfer of information outside New Zealand

In addition to disclosures permitted under this policy, we may disclose your personal information to other PwC firms within the PwC global network (PwC Network Firms).

For a list of where the PwC Network Firms are located, see PwC office locations. We may share personal information with other PwC member firms where necessary, for example for administrative purposes and to provide professional services to our clients (e.g. when providing services involving advice from PwC member firms in different territories) or for any of the purposes set out above.

PwC and other PwC Network Firms with which we exchange information may also use overseas facilities or contractors to process or back-up our information or to provide certain services to us (e.g. offshore cloud service providers). These PwC Network Firms, service providers and contractors may not be New Zealand entities or regulated by the Privacy Act, and may not be subject to privacy laws that provide the same level of protection as New Zealand's Privacy Act.

Before disclosing personal information to an overseas recipient, PwC will take reasonable steps to ensure the disclosure is permitted under IPP 12 of the Privacy Act. This may include confirming that the recipient is subject to comparable privacy safeguards, is subject to the Privacy Act, or is contractually required to protect the information in a way that overall provides comparable safeguards. Where PwC relies on your authorisation to disclose information to an overseas recipient, we will expressly inform you that the overseas recipient may not be required to protect the information in a way that provides comparable safeguards to the Privacy Act.

We will take all steps that are reasonably necessary to ensure your personal information is treated securely and in accordance with this privacy policy as well as applicable data protection laws.

Any such transfer of personal information does not change any of our commitments to safeguard your privacy and the information will remain subject to any existing confidentiality obligations.

7. Our use of Generative Artificial Intelligence tools

Where appropriate, we use Generative Artificial Intelligence ("GenAI") tools to enhance efficiency and productivity in our business processes and in the provision of professional services to our clients.

To safeguard personal information when using GenAI tools, we have implemented robust measures, including the following:

- Your personal information remains within protected Enterprise Grade environments. We only use secure, enterprise level GenAI tools.
- Your personal information is not used to train AI tools or models.

- We only upload personal information into GenAI tools where doing so complies with this privacy policy, for the purposes and grounds that we describe in sections 2 and 3 above. By using GenAI tools, we do not collect, use or hold any additional personal information, other than the personal information described in section 1 above.
- We do not allow sensitive personal information to be uploaded into GenAI tools.
- We have a Responsible AI Use policy and Business Rules for the use of AI tools, which all staff must comply with.

8 Privacy on our Web Sites and Applications

This policy also applies to any personal information we collect via our websites, including pwc.co.nz, and applications including mobile applications, in addition to personal information you provide to us directly (such as where you make a direct request to us or complete a registration form).

In order to properly manage our websites and applications, we may log certain statistics about the users of these facilities, for example the users' domains and browser types. None of this information specifically identifies an individual and it is used solely to ensure that our websites and applications provide the best possible navigational experience for users.

Cookies and web beacons are used on some PwC websites.

Cookies are small text files that are placed on your computer by the websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. If you are uncomfortable with the use of cookies, you can manage and control them through your browser, including removing cookies by deleting them from your 'browser history' (cache) when you leave the site. In most cases, you can refuse a cookie and still fully navigate the PwC websites. If you require more information on the type and use of cookies by PwC, see our Cookies Information page.

A web beacon is a clear picture file used to keep track of your navigation through a website. Along with cookies, web beacons help us gain an understanding of how users of PwC websites navigate through and process the content contained in those websites. On occasion PwC will advertise on third party websites. As part of the tracking process for advertising campaigns we may at times use web beacons to count visitors who have come to the PwC websites after being exposed to PwC advertising on a third party site.

We do not use this technology to access your personal information.

If you have registered an account with us, you will be identified by a user name and password when you log into our website or applications. The information we collect about use of our websites may be used for measuring use and performance and in assisting to resolve any technical difficulties.

Because PwC wants your user experience to be as informative and resourceful as possible, we provide a number of links to websites and embedded content operated by third parties that may also set cookies and web beacons. PwC is not responsible for the privacy practices or policies of those sites. We encourage you to review each website's privacy policy, especially if you intend to disclose any personal information via that site. A link to another non-PwC website is not an express or implied endorsement,

promotion or warranty of the products or services offered by or accessible through that site or advertised on that site.

9. Security of personal information

PwC will endeavour to take all reasonable steps to keep secure any information which we hold about you, whether electronically or in hard-copy, and to keep this information accurate and up to date. We also require our employees and data processors to respect the confidentiality of any personal information held by PwC.

PwC aims to achieve industry best practice in the security of personal information which it holds. We adhere to internationally recognised security standards and our information security management system relating to client confidential data is independently certified as complying with the requirements of ISO/IEC 27001:2013. We have a framework of policies, procedures and training in place covering data protection, confidentiality and security and regularly review the appropriateness of the measures we have in place to keep the data we hold secure.

10. Access to information

We will provide access to personal information upon request by an individual, except in the limited circumstances in which it is permitted for us to withhold this information.

When you make a request to access personal information, we will require you to provide some form of identification (such as driver's licence or passport) so we can verify that you are the person to whom the information relates. In some cases we may also request an administrative fee to cover the cost of access, where legally permitted and appropriate in the circumstances. We will tell you before proceeding.

If at any time you want to know what personal information we hold about you, you may contact us by emailing us at nz_privacy_officer@pwc.com.

11. Residents in the European Economic Area

If you are a resident in the European Economic Area, you have the following rights in relation to your personal information (where applicable):

1. **Access.** You have the right to request a copy of the personal information we are processing about you. For your own privacy and security, at our discretion we may require you to prove your identity before providing the requested information.
2. **Rectification.** You have the right to have incomplete or inaccurate personal information that we process about you rectified.
3. **Deletion.** You have the right to request that we delete personal information that we process about you, except we are not obliged to do so if we need to retain such data in order to comply with a legal obligation or to establish, exercise or defend legal claims.
4. **Restriction.** You have the right to restrict our processing of your personal information where you believe such data to be inaccurate; our processing is unlawful; or that we no longer need to process such data for a particular purpose unless we are not able to delete the data due to a legal or other obligation or because you do not wish for us to delete it.

5. **Portability.** You have the right to obtain personal information we hold about you, in a structured, electronic format, and to transmit such data to another data controller, where this is (a) personal information which you have provided to us, and (b) if we are processing that data on the basis of your consent or to perform a contract with you. Privacy Policy 493076_1 6
6. **Objection.** Where the legal justification for our processing of your personal information is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for the processing
7. **Withdrawing Consent.** If you have consented to our processing of your personal information, you have the right to withdraw your consent at any time, free of charge. This includes cases where you wish to opt out from marketing messages that you receive from us. To make a request to exercise any of these rights in relation to your personal information, please email, call or write to us using the contact information listed below in the “Introduction” and “Correction and Concerns” sections.

13. Corrections and concerns

If you believe that information we hold about you is incorrect or out of date, or if you have concerns about how we are handling your personal information, please contact us and we will try to resolve those concerns. You can direct any requests for correction or concerns to our Privacy Officer via email to nz_privacy_officer@pwc.com. If PwC becomes aware of any ongoing concerns or problems concerning our privacy practices, we will take these issues seriously and work to address these concerns. If you have any further queries relating to our privacy policy, or you have a problem or complaint, please contact our Privacy Officer. If you are not satisfied with our handling of your problem or complaint you may make a complaint to the Office of the Privacy Commissioner (<https://www.privacy.org.nz/about-us/contact/>).

14. Effect of and changes to this policy

This privacy policy was last updated on 4 June 2026, the previous date before that was 24 October 2024. This privacy policy was separated from the external privacy policy and covers employees, partners and independent contractors. PwC operates in a dynamic business environment, and we aim to review this policy annually to keep it current. We may update this privacy policy at any time by publishing an updated version here. So you know when we make changes to this privacy policy, we will amend the revision date at the top of this policy. The newly amended privacy policy will apply from that revision date. Therefore, we encourage you to review this privacy policy periodically to stay informed about how we are protecting your information. Any amended policy will apply between us whether or not we have given you specific notice of any change.