Date: December 2022
Business unit: Corporate Affairs

Confidentiality and Privacy Policy

1. Purpose

We are committed to ensuring that all our people, including our directors, employees and contingent workers, preserve and respect the confidentiality of our company, employee and customer information. Our information is a valuable corporate asset and effective dissemination, and protection, of information is important to our business success.

2. Application

This policy applies to all directors, and all employees (including any secondee, contractor or consultant) of Contact and its subsidiaries (collectively 'employees'). 'Contact' includes its subsidiaries.

It also applies to any suppliers who have access to confidential, proprietary or personal information in relation to Contact's operation, employees or customers.

3. Confidential and Proprietary information

Confidential information is information that we consider private and that is not generally available outside Contact – this includes information about our customers, employees, pricing, and strategy or general business.

Proprietary information is information that we own, develop, pay to have developed or to which we have an exclusive right.

Other than in the context of carrying out genuine business tasks, employees must not disclose or take confidential and proprietary information.

If confidential or proprietary information needs to be shared with a third party, we expect that you will consult with the Legal team to ensure that appropriate precautions are taken, such as the signing of a confidentiality agreement, and take appropriate steps to share only the minimum of what is needed or requested.

Information that is not public, and that may have an impact on our share price if disclosed, is also subject to Contact's *Market Disclosure Policy* and *Securities Trading Policy*.

4. Privacy

We expect all employees to comply with the *Privacy Principles* set out in the Privacy Act 2020 (the **Act**) in relation to all personal information (as defined in the Act) that we hold, whether that relates to customers, employees or otherwise.

The Privacy Principles cover the collection, use, access to, disclosure, storage, security and retention of personal information.

Personal information is any information about an identifiable individual, and includes:

- information that can be matched with other information to identify an individual;
- whether the information is fact or opinion;

- whether the information is true or not;
- whether the information is sensitive or not; and
- whether or not the information is publicly available.

We expect our employees who have and use personal, proprietary or confidential information will take appropriate steps to share only the minimum of what is needed or requested and ensure the security of that information (including when sharing that information internally and externally) which includes appropriate storage and may include encrypting and password protecting any personal information.

We expect all employees and suppliers who have access to, who use or collect personal information held by Contact to complete any required training modules as soon as possible after joining us, so that they understand their obligations, and refresh that training regularly. We expect our employees to ensure that any potential breach of the Privacy Principles is escalated appropriately and is brought to the attention of our Privacy Officer (who is the Chief Corporate Affairs Officer).

We expect all our employees who receive requests for access and correction will deal with those requests in accordance with the Privacy Principles and the Act. If you have any concerns or questions when dealing with a request for access or correction, please contact an Associate Privacy Officer for assistance.

We expect that where our employees are considering using an overseas person or entity to store or process personal information on Contact's behalf (for example, a new payroll provider, or a new email solution) that you contact the Legal team to determine if a further assessment needs to be undertaken to ensure compliance with the Privacy Principles. The *Offshore Disclosure Procedure* sets out more detail about what to do and when.

Privacy breaches

We expect all our employees who become aware of a privacy breach to report it in accordance with the *Privacy Breach Procedure*. A **privacy breach** is, in relation to personal information held by Contact:

- an unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information; or
- an action that prevents Contact from accessing that information on either a temporary or permanent basis; and

includes any of the things listed in the above two points, whether or not:

- it was caused by a person inside or outside Contact;
- is attributable in whole or in part to any action by Contact; or
- is ongoing.

Privacy Committee

The Privacy Committee comprises the Chief Corporate Affairs Officer (who is also the Privacy Committee Chair and Privacy Officer), General Counsel, and a representative from each of the Retail, People Experience and ICT business units.

The Privacy Committee will convene to consider a privacy breach reported to it and decide whether it should be reported to the Office of the Privacy Commissioner and affected individuals or by way of public notice. If the Privacy Committee considers the breach to be notifiable, it will ensure that the breach is reported in accordance with the Act. The decisions of the Privacy Committee shall be recorded.

5. Related documents

Our online privacy policy applies to individuals who use the Contact website or app. This policy can be viewed on our *website*.

Our general terms and conditions for residential and business customers include terms and conditions relating to privacy, and can be viewed on our *website*.

The *Privacy Breach Procedure* sets out systems and processes that Contact will follow to ensure that notifiable privacy breaches and compliance notices are appropriately managed in accordance with the Act.

The *Offshore Disclosure Procedure* provides guidance for when Contact is considering storing, processing or disclosing personal information outside of New Zealand and to ensure compliance with the Act, specifically Information Privacy Principle 12.

6. Compliance

Contact requires all of its employees to comply with this policy. Compliance with this policy will be periodically monitored by the General Counsel and Chief Corporate Affairs Officer.

Any known or suspected instances of non-compliance should be discussed with your people leader, your Leadership Team member, the General Counsel or the Chief Corporate Affairs Officer. Alternatively, any employee who is aware of a breach of this policy can take action in accordance with Contact's *Whistleblowing Policy*.

7. Document control

Approved:	December 2022	**Document owner:**	Chief Corporate Affairs Officer