Privacy Policy

Oxygen.co.nz Limited & Oxygen Strata Limited

OXYGEN

Contents

Policy

How Oxygen.co.nz Limited / Oxygen Strata Limited (Oxygen) collect, use, disclose, and protect personal information is important to our business. We all have a part to play ensuring we comply with our privacy obligations in relation to the use and protection of personal information and our goal to be completely transparent about what we do with personal information.

Under the Privacy Act 2020, there are 13 Information Privacy Principles (IPPs) our business must comply with. When collecting, using and disclosing, and protecting personal information of any description, we must do so in accordance with the IPPs. The IPPs can be summarised as follows:

1. Only collect information the business needs.
2. Wherever possible, get the personal information directly from the individual.
3. Be transparent about what you are going to do with the personal information.
4. Be fair about how you get it.
5. Keep personal information secure.
6. Enable personal information to be accessed by the person it relates to.
7. Enable personal information to be corrected if it is incorrect.
8. Ensure personal information is correct before you use it.
9. Dispose of personal information securely once you no longer need it.
10. Only use personal information for the reason it was collected.
11. Only share personal information if you have a good reason.
12. Only send it overseas if it will be adequately protected.
13. Only use unique identifiers when it is clearly allowed.

This Privacy Policy sets out how our business collects, uses, discloses and protects the personal information we deal with in a way that complies with the Privacy Act 2020. The Employee/ Contractor Privacy Statement (Appendix B) sets out how we collect and use the personal information of our employees and contractors. We make a client Privacy Statement and Privacy Policy available to clients and prospective clients, which sets out how our business deals with client information.

Failure to comply with this Privacy Policy

All employees and contractors should be aware that a failure to comply with this Privacy Policy, including any policies, processes and controls which are put in place under it, will be investigated and may lead to disciplinary action being taken.

Procedure

Collecting personal information

Personal information is defined in the Privacy Act 2020 as information about an identifiable individual (a natural person as opposed to a company or other legal entity).

Types of personal information we collect

Our business collects personal information from:

- Employees;
- Prospective employees;
- Contractors;
- Authorised bodies;
- Outsource providers;
- Clients; and
- Prospective clients.

We only collect information we need. Where practicable, we collect personal information directly from the source, eg; directly from the employee. We only keep personal information for as long as it is necessary. The amount of time that we hold the personal information for (retention period) varies, depending on the nature of the personal information. The retention periods are set out in the Information Register (Appendix A).

All employees receive training to enable them to understand how the Privacy Act 2020 impacts on how we provide our services to clients and manage our business. Employees also receive training on the IPPs, how they impact the process of collecting information, and the ways in which they can and cannot collect personal information in their roles.

Storage and protection of personal information

We only keep personal information for as long as it is necessary. The amount of time that we hold the personal information for (retention period) varies, depending on the nature of the personal information. The retention periods are set out in the Information Register (Appendix A). Our records are systematically checked through our CRM software to ensure that personal information is only kept while there is a lawful or legitimate business purpose.

Most of the data we collect through our business (including most personal information we collect) is stored electronically. We take all reasonable steps to keep it secure and prevent unauthorised disclosure. Employees and contractors also play an important role in keeping the information safe. All our employees and contractors are required to adhere to Oxygen policies, processes and controls to help meet our Privacy Act 2020 obligations. This includes keeping passwords and devices secure,

adhering to email and internet usage guidelines and being subject to employee monitoring, as set out in our IT and cybersecurity policies.

Privacy and remote working (working from home)

Remote working introduces additional risks in relation to potential breaches of privacy. We take all reasonable steps to ensure personal information is protected in these circumstances, including:

- Requiring a trusted WiFi network to be used (eg; home WiFi);
- Having multi-factor authentication enabled;
- Locking out a user after numerous failed logins;
- Ensuring staff can only access information they need;
- Storing devices in a safe location;
- Ensuring work conversations are not overheard by other members of the household;
- Locking devices when they are not in use; and
- Increased vigilance of unexpected emails.

If there is a privacy breach

We work hard to keep all personal information safe. However, despite applying strict security measures and following industry standards to protect personal information, there is still a possibility that our security could be breached.

If you are aware of a privacy breach, where there is a loss or unauthorised access or disclosure of personal information, whether or not you think it is likely to cause serious harm, you must notify the Privacy Officer as soon as you become aware of the breach. This will allow us to:

- Seek to quickly identify and secure the breach to prevent any further breaches and reduce the harm caused by the breach;
- Assess the nature and severity of the breach, including the type of personal information involved and the risk of harm to affected individuals;
- Advise and involve the appropriate authorities where criminal activity is suspected;
- Where appropriate, notify any individuals who are affected by the breach (where possible, directly);
- Where appropriate, put a notice on our website advising our clients of the breach; and
- Notify the Privacy Commissioner.

All employees receive training to enable them to identify a privacy breach, how to reduce the risk of a privacy breach occurring and how to respond to a privacy breach if one does occur.

We maintain a Breaches Register (Appendix C) to record all privacy breaches that occur in our business, whether or not they pose a risk of serious harm or require us to notify any external parties.

It is important that you notify the Privacy Officer as soon as you become aware of any privacy breach, so that the breach can be logged on the Breaches Register and any necessary further action can be considered.

Disclosure of personal information

We only disclose personal information to others outside Oxygen where:

- It is necessary to enable us to achieve the purpose that we collected the information for;
- We are required or authorised by law or where we have a public duty to do so;
- We have received express consent for the disclosure from the person the information relates to, or consent can be reasonably inferred from the circumstances; or
- We are permitted to disclose the information under the Privacy Act 2020.

Please contact the Privacy Officer if you are not sure whether you are permitted to disclose personal information either internally or externally. We have legal obligations to maintain personal information to disclose to regulatory and similar bodies. The Information Register (Appendix A) outlines internal and external sharing of personal information.

Before entering into an agreement with an outsourcing provider or other third party, we undertake due diligence checks of the third party. All agreements that are entered into with third parties include provisions to ensure personal information is dealt with as required by the Privacy Act 2020.

Sending personal information out of New Zealand

We may send personal information outside New Zealand, including to overseas members of Oxygen related companies and overseas service providers or other third parties who process or store our information, or provide certain services to the business.

Where we do this, it does not change any of our commitments to safeguard privacy. We must make sure that appropriate security and information handling arrangements are in place and the information remains subject to confidentiality obligations.

All employees receive training about their Privacy Act 2020 obligations when sending personal information overseas and also our business' policy on when this may be done and the processes that must be followed before the information is sent.

All countries have different privacy laws and information protection standards. If we need to send personal information outside of New Zealand, our Privacy Officer will undertake due diligence to confirm this is permitted. The Information Register (Appendix A) sets out which external

organisations we can share personal information with. You can gain guidance from the Privacy Officer if you are unsure about whether you can send personal information outside of New Zealand.

Accessing and correcting personal information

Every person has a right to access personal information that is held about them and ask for it to be corrected if they think it is wrong. Our business has a legal duty to respond to requests for access to information or correction of that information within 20 working days of receiving the request, although our policy is to respond to the request as soon as possible.

If an employee or contractor receives a request from a person who wants to access the personal information the business holds about them, or make a correction to it, they need to send all the details of the request, along with the individual's contact details to the Privacy Officer as soon as possible after receiving it. The Privacy Officer will then follow the process set out below.

Access/Correction request process

Before processing the request, the Privacy Officer may contact the relevant individual to verify their identity, confirm the request and advise the individual of any charges that apply. The Privacy Officer will then take steps to provide the individual with access to their information, take steps to update or change the requested information, or otherwise address the query within a reasonable period after the request is received.

There are some circumstances in which our business is not required to give an individual access to their personal information or correct it upon their request. If one of these circumstances applies, the Privacy Officer will let the individual know the reasons for the refusal, unless the law prevents them from doing so. If a request to correct or delete personal information is refused, the individual has the right to request that a statement be associated with their personal information, noting that they disagree with its accuracy. We are only able to delete or remove an individual's personal information from our records if we are not required to hold the information to satisfy any legal, regulatory, or similar requirements. If the Privacy Officer refuses a request to access, correct or delete personal information, the individual will be provided with information about how they can make a complaint about the refusal.

Complaints

We have a strict timeframe for responding to any privacy related complaints received by our business. Our policy is to acknowledge all complaints within three working days of their receipt, and we aim to resolve complaints within five working days, but some take longer to resolve.

If an employee or contractor receives a privacy related complaint, they must contact the Privacy Officer and send them all relevant details of the complaint as soon as possible. The Privacy Officer will then contact the individual to acknowledge the complaint and work to resolve the complaint as quickly as possible.

Controls

- Cybersecurity policy
- IT policy
- Training and development policy
- Client onboarding policy
- Recruitment and selection policy
- Job descriptions
- Outsourcing policy and due diligence checklist
- Employment agreements
- Authorised body agreements
- Independent contractor agreements
- Business continuity plan

Appendix A – Information Register

Type of personal information	Person respsonsible	Purpose of having information	Where is it stored	Retention period	Internal sharing	External sharing
Current employees and contractors	Assistant Accountant	Performance of contract and to meet legal obligations	SharePoint, Cloud based system like iPayroll	7 years after employment ends	Managers	CPD provider, meeting legal obligations
Past employees and contractors	Assistant Accountant	Meet legal obligations	SharePoint	7 years after employment ends	Managers	Meeting legal obligations
Prospective employees and contractors	Assistant Accountant	To employee or engage the services of the contractor	SharePoint	7 years after employment ends	Managers	CPD provider, meeting legal obligations
Client records	Compliance Manager	To comply with current legislation, to provide services requested from us.	CRM cloud-based system	7 years	Salespeople, sales administrators	Third parties who enable us to provide you with our services such as CRM provider, auditor.
Prospective client's personal information	Compliance Manager	To comply with current legislation, to provide services requested from us.	CRM cloud-based system	7 years	Salespeople, sales administrators	Third parties who enable us to provide you with our services such as CRM provider, auditor.
Third parties	Assistant Accountant / Compliance Manager	To conduct business	SharePoint, cloud-based system	7 years	Relevant team members of Oxygen	Meet legal obligations

Appendix B – Employee & Contractor Privacy Statement

Oxygen collects and processes personal information relating to its employees and contractors to manage its working relationships with those people. This personal information may be held in paper and/or electronic format.

Oxygen is committed to:

- being transparent about how it handles your personal information;
- protecting the privacy and security of your personal information; and
- meeting its obligations under the Privacy Act 2020.

This Employee/Contractor Privacy Statement applies to all current and former employees and contractors that have worked with us since 1993. This statement does not form part of any contract of employment or authorised body agreement or contractor agreement.

Oxygen has appointed a Privacy Officer to oversee its compliance with the Privacy Act 2020. If you have any questions about this Employer/Contractor Privacy Statement or about how we handle your personal information, please contact either Fiona Paget – Privacy (Compliance) Officer 027 562 6481 or fiona@oxygen.co.nz

Oxygen is responsible for and must be able to demonstrate compliance with the Information Privacy Principles (IPPs).

The type of personal information we collect about you

Personal information is any information about an individual from which that person can be directly or indirectly identified. Oxygen collects and uses a range of personal information about you, including:

- Your contact details
- Your emergency contact details/next of kin
- Your date of birth
- Your gender
- Your marital status and dependants
- The start and end date of your employment
- Recruitment records
- Your salary
- Your IRD number
- Bank account details, payroll records, tax details
- Disciplinary records
- Leave records, including holiday and sickness details
- Information about your use of IT systems
- Immigration Status (if applicable)

How we collect your personal information

Oxygen may collect personal information about employees and contractors in a variety of ways. It is collected during the recruitment process, either directly from you or sometimes from a third party, such as a recruitment agency. We may also collect personal information from other third parties, such as reference from former employers, information from credit reference agencies and criminal record checks.

Using and disclosing your personal information

We will only use your personal information when the law allows us to. We will use your personal information in one or more of the following circumstances:

- So we can perform the employment or contactor agreement we have entered into with you.
- So we can comply with our legal obligations.
- The purpose for which we are using your personal information is to:
- Enable us to maintain accurate and up to date employee and contractor records and contact details
- Run recruitment processes and assess your suitability for employment, engagement or promotion
- Comply with our legal and regulatory obligations
- Administer the contract we have entered into with you
- Ensure you are paid correctly
- Ensure compliance with tax requirements
- Operate and maintain a performance management system
- Record and assess your education, training and development needs
- Plan for career development and succession
- Manage, plan and organise work
- Enable effective workforce management
- Operate and maintain leave procedures, including annual leave, sick leave, maternity leave etc.
- Ascertain your fitness to work
- Meet our obligations under health and safety legislation
- Monitor use of our IT procedures to ensure compliance with IT related policies
- Ensure network security and prevent unauthorised access to systems
- Ensure effective HR processes
- Ensure adherence to Oxygen policies and procedures
- Obtain insurance (e.g. professional indemnity insurance)

What if you fail to provide personal information?

If you fail to provide certain personal information when required, we may not be able to perform the contract we have entered into with you, or we may be prevented from complying with our legal obligations. You may also be unable to exercise your legal or contractual rights.

Change of purpose

We will only use your personal information for the purpose for which it was collected. If we need to use your personal information for a purpose other than for which it was collected, we will provide you with information about the new purpose and any additional relevant information prior to using your personal information in a new way. This will give you the opportunity to revoke your consent to the new use.

Access to your personal information

Your personal information may be shared internally within Oxygen, including with members of the HR department, payroll staff, your manager, other managers and IT staff, if access to your personal information is necessary for them to perform their roles.

Oxygen may also share your personal information with third parties and/or outsource providers (and their designated agents), including:

- Recruitment agencies for the purpose of conducting pre-employment checks
- Payroll providers
- KiwiSaver providers
- IT services
- External auditors
- Professional advisers, such as lawyers and accountants

Oxygen may also share your information in the context of a potential sale or restructuring of the business. In those circumstances your personal information will be subject to an agreement of confidentiality.

Protecting your personal information

Oxygen has put in place measures to protect the security of your personal information. It has internal policies, procedures and controls to try and prevent your personal information from being accidently lost, destroyed, altered or disclosed, or used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, contractors and third parties who need to access your personal information in order to perform their work duties and responsibilities. You can obtain further information from the Privacy Officer.

It is important that the personal information we hold about you is accurate. Please keep us informed if your personal circumstances change, e.g. you change your home address or phone number.

You have the right to:

- Request access to your personal information
- Request correction of your personal information

If you wish to access your personal information or make any correction, please contact the Privacy Officer.

Appendix C - Breaches Register

Summary of breach	Cause of the Breach	Date breach occurred	Date of awareness of the breach	Reported to Privacy Commissioner	Individuals notified or Public Notice Issued	Current Status
eg; email sent to wrong client with attached SOA	eg; human error	[Insert date]	[Insert date]	[Yes/No]	[Yes/No]	eg; closed

OXYGEN

Life just got better.

oxygen.co.nz