

<p><b>Application of Policy:</b></p>	<p>Global</p> <p>This Code sets out the minimum requirements for the Group. Where the Group operates in a jurisdiction that imposes a higher standard, or a member of the Group has adopted its own policy on a matter covered in this Code which adopts a higher standard, those local standards or the local policy are deemed to be incorporated into and supplement this Code as it applies in that jurisdiction or to that particular member of the Group and in the event of conflict supersede this Code.</p>
--------------------------------------	--

**Definitions:** Capitalised terms used throughout this Code are defined in paragraph 15.

## 1. Overview

This Code is a framework of guiding principles and standards to be followed by all Personnel in the performance of their duties. The aim of this Code is to articulate the principles, ethical standards and standards of behaviour expected of all Personnel. This Code is supported by the Group’s policies and procedures, including those located in the Corporate Governance Manual.

Personnel are expected to read this Code, understand their obligations and act consistently with the principles set out below at all times. This Code applies whenever Personnel represent the Group, which includes in the workplace and anytime they are, or are perceived to be, representing the Group, even if it is outside of the workplace or regular working hours. This includes Group functions, conferences, out-of-hours work activities and social media.

All Personnel have a responsibility to uphold the reputation of the Group and provide the best possible service to its stakeholders.

## 2. Principles

All Personnel are expected to abide by the following principles at all times:

- (a) act with integrity and transparency in respect of all stakeholders;
- (b) act in accordance with the Statement of Values and in the best interests of the Group;
- (c) act in compliance with laws and regulations and the Group’s policies and procedures;

- (d) identify and manage conflicts of interest responsibly;
- (e) treat other Personnel with respect and value diversity;
- (f) provide a safe working environment;
- (g) respect and maintain privacy and confidentiality of information and accuracy of business records; and
- (h) respect the Group's resources and information systems.

### 3. Act with integrity and professionalism when performing work duties

Integrity and professionalism are core to the Group's business and should guide all of the decisions made by Personnel in relation to their work. Acting with integrity and professionalism means being honest, respectful, truthful, sincere, fair and performing duties to the highest standards.

Personnel are expected to uphold these traits at all times in the course of their work which are integral to maintaining the trust of the Group's investors, service providers, colleagues and all other stakeholders, as well as the communities in which the Group operates.

Personnel should not engage in unconscionable or dishonest conduct, conduct that is misleading or deceptive, or provide false or misleading information when preparing reports or other materials.

Improper conduct may expose the Group to legal liability or reputational damage.

### 4. Act in accordance with the Statement of Values and in the best interests of the Group

Personnel must act in accordance with the Statement of Values at all times in the performance of their roles. The Group has developed its Statement of Values to align with its purpose and strategic objectives and to both drive and reflect the culture it strives to embed in the organisation.

In the performance of their roles personnel must act in the best interests of the Group and at all times in accordance with the legal and regulatory obligations of any member of the Group and not in their own interests. The procedure to identify and manage conflicts of interest responsibly is set out in paragraph 6.

### 5. Act in compliance with laws and regulations and the Group's policies and procedures

Personnel must be familiar with and comply with all laws and regulations applicable to their role. Failure to comply with laws and regulations can result in both Personnel and the Group facing criminal sanctions or other serious consequences.

Personnel must also comply with the Group's policies and procedures, including those found in the Corporate Governance Manual. Personnel should talk to their supervisor if they are unsure about the policies and procedures which apply to them. If necessary, you can seek the advice of the Legal, Compliance and Risk team.

Conduct which may be in breach of applicable laws and regulations or the Group’s policies and procedures should be reported to your team leader and escalated to the Head of Risk and Compliance. The Whistleblower Policy provides protection for Personnel who disclose malpractice, misconduct or conflicts of interest.

### 5.1. Anti-bribery and corruption

The Group has a zero-tolerance policy for bribery and corruption in any form and is committed to maintaining a high standard of integrity in its operations and at all times strives to operate in an ethical manner and in accordance with the Statement of Values and the Code of Conduct. Bribery and other types of corrupt conduct are serious criminal and civil offences for both the applicable member of the Group and any individuals involved and have potential to cause significant reputational damage to the Group. The Group will conduct business with integrity and will comply with applicable laws and regulations, including the FCP Laws. Bribery and other corrupt practices in any form are expressly prohibited.

For further information, refer to the Anti-Bribery and Corruption Policy (**ABAC Policy**).

### 5.2. Inside Information

Inside information is information about an entity which is both material and non-public (**Inside Information**). It is an offence to trade using Inside Information, or communicate Inside Information to others who will, or are likely to, trade on the Inside Information. Telling someone or conveying Inside Information to them is a crime called “tipping”.

Personnel must never deal (or communicate or pass on inside information to others who might deal) using confidential information they have obtained at the Group in the course of their work (see section 9 below).

In addition, Personnel must never deal (or communicate or pass on Inside Information to others who might deal) in Company securities while in possession of ‘Inside Information’ in relation to those securities. Additional restrictions on dealing in Company securities apply to certain persons within the Group. For further information, refer to the Securities Trading Policy.

### 5.3. Continuous disclosure

The Company must ensure that, for as long as its securities remain admitted to trading on ASX, it provides the market with relevant information in a timely and balanced manner in accordance with applicable laws and regulations. Personnel have a responsibility to escalate information requiring disclosure to one of the Disclosure Officers and should be familiar with the Continuous Disclosure Policy.

## 6. Identify and manage conflicts of interest responsibly

A ‘conflict of interest’ arises when a member of Personnel has a direct or indirect (through a family member, friend or associate), professional or personal interest in a matter, investment, service provider or transaction:

- (a) in which they know or believe that the Group has an interest; or

- (b) which is inconsistent with the interests of the Group and/or the Group's stakeholders; or
- (c) Shareholders, to the extent of their interests as a Shareholder.

This direct or indirect interest would either make it difficult for the member of Personnel to fulfil their duties properly or would create an appearance of impropriety that could undermine stakeholder or public confidence in the Group.

An actual interest is one known to exist. A potential interest is one believed to be under consideration or discussion. A perceived interest is where other people might reasonably think that a person has been compromised.

Examples of conflicts of interest include:

- (a) holding business interests or employment outside of the Group;
- (b) close affiliations or family connections with service providers, suppliers or contractors;
- (c) offering or accepting gifts and hospitality outside of the boundaries of the Group's policies and this Code;
- (d) pursuing Group business opportunities for personal gain; or
- (e) influencing business decisions concerning a partner, close relative(s) or friend(s).

Personnel should avoid participating in activities that involve a conflict of interest between their personal interests and their duties and obligations to the Group or which a reasonable person would perceive as involving such a conflict of interest.

To manage conflicts of interest Personnel must:

- (a) disclose any actual, potential or perceived conflicts of interest to their team leader, or if inappropriate to the Managing Director, for consideration. The team leader or Managing Director should escalate the matter to the Head of Compliance and Risk who will ensure the issue is properly reviewed and provide information about the appropriate manner in which to deal with the conflict;
- (b) disclose any participation in outside business activities, including non-Group work, business ventures, director appointments (other than to the board of a non-trading family company), partnerships or other interests which have the potential to create a conflict of interest. Disclosure should be at the time of appointment with the Group, otherwise, approval should be sought from a Chief Investment Officer or Executive Director for the applicable region, or if inappropriate from the Managing Director, for consideration before participating. The Head of Compliance and Risk must be notified of any disclosure;
- (c) not solicit or accept money, gifts, favours or entertainment which might influence or be seen to influence their business judgement. If Personnel accept any money, gifts, favours or entertainment exceeding the relevant regional thresholds in the ABAC Policy, relevant details of the transaction must be disclosed in accordance with the

ABAC Policy; and

- (d) deal with all stakeholders fairly and on an arm's length basis.

In addition to properly dealing with personal conflicts of interest, Personnel have a responsibly to assist with identifying and managing any conflicts the Group faces in the course of its business in accordance with applicable policies and procedures.

## 7. Treat other employees with respect and value diversity

The Group does not tolerate bullying, discrimination, harassment, victimisation or unreasonable or unlawful behaviour. All Personnel are responsible for eliminating such practices in the workplace.

The Group is committed to diversity and equal opportunities in the workplace. Personnel should be familiar with the Diversity Policy.

## 8. Provide a safe working environment

As set out in the Health and Safety Policy, the Group is committed to providing a safe and healthy working environment and complying with all relevant laws and regulations relating to health and safety in the workplace.

Personnel are expected to:

- (a) report any health and safety issues that come to their attention;
- (b) abide by Group health and safety policies and procedures which apply to them and follow safety instructions; and
- (c) comply with Group policies on alcohol and smoking in the workplace.

The Group has a zero tolerance policy towards illegal drug use and possession and the misuse of prescription drugs on its premises, when conducting business on the Group's behalf or at Group work-related functions or activities.

## 9. Respect and maintain privacy and confidentiality of information

Personnel may come across confidential information concerning the Group's stakeholders and other third parties in the course of their work. It is vital that all Personnel respect the trust placed in the Group by those people. Their confidential information must not be used or disclosed, except with their authorisation and where the use or disclosure is authorised by law.

Similarly, Personnel may come across confidential information concerning the Group, such as strategic or financial information, commercial arrangements or intellectual property.

Personnel must at all times:

- (a) use confidential information solely for the proper performance of their duties; and
- (b) preserve the confidentiality of the Group's confidential information and only disclose it to other Personnel or authorised recipients who need to know the information, or

as required by law.

Personnel are bound by the confidentiality obligations outlined above and in their employment agreement (or other agreement concerning their engagement) even after leaving the Group.

### 9.1. Public statements

Personnel must not, without authority, directly or indirectly state that they are representing the Group or its public position in respect of any matter.

All public statements to be made on behalf of the Group must be authorized by the Managing Director in accordance with the External Communications policy. This also includes when Directors or senior executives are required or intend to make public statements in relation to matters under their control. Such statements should be discussed with or otherwise authorized by the Managing Director in order to allow for coordination of the Group's public stance in relation to that matter and to ensure the disclosure is not in breach of the Continuous Disclosure Policy.

Personnel must not directly or indirectly engage in any activity which could by association cause the Group public embarrassment or damage.

Personnel should always cooperate fully with any internal or external reviews or investigations, including those conducted by external auditors and regulators. You must not hinder or obstruct any investigation or destroy, discard, withhold or alter records pertinent to any investigation.

### 9.2. Privacy

The Group abides by laws governing privacy of personal information obtained in the course of its business.

Personnel are expected to be familiar with and comply with the Group's Privacy Policies and Procedures.

## 10. Respect the Group's resources and information systems

All Personnel must only use Group property, funds, facilities and services for authorised purposes and not for personal benefit or the benefit of unauthorised third parties including being sensitive to the impact our resources and information systems may have on the environment that is relevant to the industry in which we operate.

Any transactions (including disposals) involving Group property must be approved by a Chief Investment Officer or Executive Director for the applicable region or the Group CFO and accurately recorded in financial records.

The unauthorised removal of Group equipment, supplies and other resources is considered to be theft.

### 10.1. Electronic equipment

Laptop and desktop computers, mobile phones, tablets and associated devices are issued

to Personnel to assist them in fulfilling their duties and responsibilities. Electronic equipment and software assigned to Personnel remains the property of the Group. The Group may at any time request Personnel to return any electronic equipment issued to them for maintenance and security checks.

Accessing, storing or disseminating any material that is illegal, obscene, discriminatory, defamatory, hateful or that may annoy, harass or intimidate another person is prohibited. The downloading of unauthorised software is not permitted. Before linking personal devices to the Group's information systems authorisation must be obtained from the Group's IS Manager.

By using electronic equipment provided by the Group, Personnel agree to abide by all Group policies and procedures relating to the use of that equipment. Failure to comply with the Group's policies and procedures may result in access to electronic equipment being restricted and, in some cases, disciplinary action being taken.

## 10.2. Electronic communications

Personnel must comply with any applicable Group policies and procedures relating to electronic communications and surveillance.

## 10.3. Social media/networking

Personnel must use social media and networking sites in accordance with this Code and applicable Group policies and procedures.

## 11. Breaches of the Code

The Group takes compliance with this Code very seriously. Failure to comply with this Code may result in one or more of the following:

- (a) a formal warning;
- (b) additional training;
- (c) performance management;
- (d) termination of employment or contractual arrangements; or
- (e) civil or criminal prosecution.

Personnel are strongly encouraged to report any suspected breaches of this Code. Breach reports should be made to the Head of Compliance and Risk. Personnel should ensure they are familiar with the Whistleblower Policy, which protects Personnel who disclose malpractice, misconduct or conflicts of interest from detrimental consequences as a result of making the report.

The Managing Director must promptly report any material breaches of this Code to the Board.

## 12. Initial and Annual Attestation

This Code will be provided to all Personnel when joining the Group. Personnel will be

required to make an attestation agreeing to compliance with the Code upon employment and annually thereafter.

Compliance with the Code is considered to be a condition of employment with the Group.

### 13. Training and Monitoring

The Group will provide initial training in relation to this Code and thereafter on a periodic basis. The Group will put in place compliance monitoring programs to review the Group's compliance with the requirements of this Code.

### 14. Review and Amendment of this Code

This Code will be reviewed periodically by the Board to check that it is operating effectively and whether any changes are required.

Any amendments to this Code, other than updates for changes in the Group's branding or position titles, must be approved by the Board.

### 15. Definitions

Defined terms used in this Code have the following meanings:

<b>Term or Abbreviation</b>	<b>Definition and Explanation</b>
<b>Board</b>	means the board of Directors.
<b>CFO</b>	means the chief financial officer of the Company.
<b>Code</b>	means this code of conduct.
<b>Company</b>	means Omni Bridgeway Limited (ABN 45 067 298 088).
<b>Company Secretary</b>	means a person appointed as, or to perform the duties of, secretary of the Company.
<b>Director</b>	means a director of the Company.
<b>Disclosure Officers</b>	means the Managing Director, the Company Secretary and the CFO.
<b>Executive Director</b>	means an executive Director.
<b>Group</b>	means the Company and its related bodies corporate (as that term is defined in section 9 of the <i>Corporations Act 2001</i> (Cth)).
<b>Managing Director</b>	means the managing director of the Company or such equivalent office.
<b>Personnel</b>	means all full-time, part-time or casual staff, consultants, contractors, secondees and directors of or to the Group.



<b>Term or Abbreviation</b>	<b>Definition and Explanation</b>
<b>Shareholders</b>	means shareholders of the Company.
<b>Statement of Values</b>	means the values and characteristics applicable to Personnel set out on the Company’s intranet, as updated from time to time.

**This Code was approved by the Board to be effective on 28 April 2023.**