



Code of Conduct

IPD Group Ltd (ACN 111 178 351) (Company)
Adopted by the Board on **14 September 2023**
(amended on 22 May 2024)

IPD Group Limited
ABN 12 111 178 351
www.ipdgroup.com.au

HEAD OFFICE
43 Newton Road, Wetherill Park, NSW, 2164
PO Box 6422, Wetherill Park, NSW, 1851
Tel: (02) 9645 0777
Fax: (02) 9645 1608

1. Purpose and application

1.1. Purpose of this code

IPD Group Ltd and its subsidiaries (**Company**) are committed to the highest level of integrity and ethical standards in all business practices, including strict compliance with state and territory legislation and international anti-corruption and anti-bribery standards. This code of conduct sets out the standards of conduct expected of our business and people, taking into account the Company's legal and other obligations to its stakeholders.

The board of directors of the Company (**Board**) has endorsed this code. The Board and management believe that the Company's commitment to this code will maintain the confidence of the Company's key stakeholders in the Company's integrity.

For the avoidance of doubt this code applies to the Company and all of its subsidiary companies.

1.2. Application of this code

This code applies to all directors of the Board, as well as all officers, employees, contractors, consultants, other persons that act on behalf of the Company, and associates of the Company (for the purpose of this code, collectively referred to as **Personnel, you**).

Personnel are expected at all times to act consistently with this code of conduct, current community standards and in compliance with all relevant law. This code operates in conjunction with all other Company policies and procedures.

It is essential that all Personnel are familiar with this code, which is available on the Company's website and intranet.

Suppliers and other interested parties are expected, to the extent possible, to adhere and comply with this code in their dealings with the Company.

2. Our values and commitments

The Company's core values and commitments are:

- (a) **People first** – We respect every individual, valuing their unique perspectives and contributions.
- (b) **Knowledge is our key** – Knowledge is our greatest tool in helping customers thrive and succeed.
- (c) **Earn customers for life** – Striving for lifelong customers, one interaction at a time.
- (d) **Stronger together** – With collaboration, we can overcome any challenge together.
- (e) **Own it** – We take responsibility for our actions to drive positive change.
- (f) **Courage to evolve** – We embrace new opportunities, challenge norms, and evolve together in the pursuit of a sustainable tomorrow.

3. Our ethical standards and policies

3.1 Standards of Behaviour

Personnel are required to:

- (a) act in accordance with the Company's stated values and commitments;
- (b) abide by all applicable laws, regulations and rules, and the Company's policies, and procedures (as amended from time to time);
- (c) comply with all lawful and reasonable directions given by the Company;
- (d) perform all duties and responsibilities competently, diligently, and to the best of their ability;
- (e) devote the whole of their time during ordinary business hours to carry out their duties and not engage in excessive personal activities;
- (f) be courteous, respectful, and considerate in all communications;
- (g) display professionalism at all times;
- (h) work cooperatively and collaboratively with others to achieve common goals and a harmonious work environment;

- (i) avoid engaging in gossip or any form of conduct that may cause unwanted offence or embarrassment;
- (j) not engage in any fraudulent, dishonest, illegal, unethical or improper behaviour;
- (k) be truthful in all dealings and not make any false or misleading statements;
- (l) not engage in unlawful bullying, harassment, discrimination, or victimisation;
- (m) not engage in verbal or physical aggression;
- (n) comply with all health and safety requirements;
- (o) deal with customers and suppliers fairly;
- (p) not take advantage of the property or information of the Company or its customers for personal gain or to cause detriment to the Company or its customers;
- (q) take all steps necessary to ensure the protection of the Company's business, assets, premises, confidential information and resources;
- (r) report all information required by the Company accurately and honestly.

3.2 Conflicts of interest

A conflict of interest exists where loyalties are divided. For example, if you or your relatives or associates have a personal or commercial interest which may interfere, or be perceived to interfere, with the performance of your duties and responsibilities to the Company, making it difficult to perform your role objectively and effectively. It is imperative that you are able to manage a conflict of interest when it arises.

Personnel must act in the best interests of the Company. To safeguard the confidence of the Company's key stakeholders in the Company's integrity, it is paramount that personnel do not allow personal interests or the interests of relatives or associates to conflict with the interests of the Company. Personnel must avoid participating in decisions and activities which may conflict, or be perceived to conflict, with their duties and responsibilities to the Company.

Personnel are required to state any potential conflicts of interest as soon as they become aware. Employees are required to complete the [Conflict of Interest Declaration Form](#) on an annual basis and provide it to HR.

3.3 Financial interests in other businesses and outside memberships

Personnel must not enter into any arrangement or participate in any activity that would conflict with the Company's best interests or would be likely to negatively affect the Company's reputation.

Personnel must not be involved in any other company or business or organisation as director, agent, employee or consultant, whether paid or unpaid, if there is a possibility that their personal interests could conflict, or be perceived to conflict, with those of the Company unless they obtain approval first from the Chief Executive Officer or the Board (if they are a director).

Personnel involved in a conflict or possible conflict, or who become aware of a conflict, must tell their manager, HR, Chief Executive Officer or the Board (if they are a director) as soon as possible.

3.4 Corporate opportunities, benefits and ownership of work

Personnel must not use Company or customer property, or information, their position or opportunities which arise from these to improperly gain benefit for themselves or for another party or to cause detriment to the Company or its customers.

Personnel have an obligation to avoid all financial, business and other arrangements which may be opposed to the interests of the Company, or which may place them in a competitive position with the Company.

The product of any work performed with the Company, or on behalf of the Company, or using Company property (including all intellectual property rights created in connection with that work) belongs to the Company.

3.5 Anti-bribery and gifts

A number of countries have strict laws against bribery and corruption. The anti-bribery laws of some countries including the United States and Australia can apply to things done in other countries (i.e. wide-reaching extraterritorial effect). The Company must comply with and uphold all laws against bribery, corruption and related conduct applying to the Company in all the jurisdictions where the Company operates.

Personnel must deal fairly with the Company's shareholders, customers, suppliers, competitors, employees and anyone else with whom they have contact in the course of performing their work duties. Personnel must not take unfair advantage of anyone through bribery or other corrupt practices, manipulation, concealment, abuse or privileged information, breaching privacy or confidentiality requirements, deception, misrepresentation of facts or any other unfair dealing practice.

The Company is committed to adopting effective systems to counter bribery and related improper conduct and to monitoring and enforcing these systems. Accordingly, the Company has implemented a strict Anti-Bribery & Anti-Corruption Policy that applies to all individuals working at all levels and grades within the Company including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located.

The Company's [Anti-Bribery & Anti-Corruption Policy](#) is available on the Company's website and on the intranet.

3.6 Politicians, government officials and lobbying

All dealings with politicians and government officials which relate to the Company and its business activities must be conducted at arm's length and with the utmost professionalism, to avoid any perception of attempts to gain advantage or to improperly influence the outcome of an official decision.

Personnel must not make any donation or other financial contribution to any political party or candidate for an election or sponsor any organisations (other than in a purely personal capacity) without seeking and obtaining prior approval from the Chief Executive Officer. Under this code, all payments to government officials to secure an advantage, including payments to expedite or secure the performance of routine action, are prohibited.

Without specific authorisation from the Company, personnel must not engage in any lobbying of political officials, elected or appointed. Lobbying activity generally includes the attempt to persuade such officials to follow a particular course of action or policy or attempts to influence the passage or defeat of legislation and may trigger registration and reporting requirements. In many jurisdictions, the definition of lobbying activity is extended to cover efforts to induce rule making by executive branch agencies or other official actions of agencies, including the decision to enter into a contract or other arrangement.

The Company encourages its Personnel to take an active role in government processes. However, any participation in a political process is to be undertaken as an individual and not as a representative of the Company. Do not engage in lobbying activities on behalf of the Company without prior consultation with the Chief Executive Officer and Chairperson.

3.7 Confidentiality

In the course of the Company's business, personnel will have access to business or personal information about the affairs of the Company, its clients, Personnel, suppliers and business partners. It may include business strategies, competitive analysis, financial plans and forecasts, employee information, supplier information and pricing.

Each of the parties expects the confidential nature of the information they have given in good faith to be respected.

Personnel must keep confidential information acquired during employment with the Company, or acting on behalf of the Company, confidential, both during and after their employment or engagement ceases. The Company encourages Personnel to store business records and confidential information securely. Anyone who uses the Company's systems or has access to the Company information (including access through personal devices such as laptops or mobile devices) shares responsibility for the security of those systems and information and must protect Company property – including data, information and systems – from theft, carelessness, misuse, unauthorised access and vulnerability to cyber attack.

Personnel must not access or request or make improper use of or transfer or disclose confidential information to anyone else except as required by their position or as authorised or legally required. If it inadvertently comes into possession it should be returned immediately. If required by an authority to provide confidential information which has not been otherwise authorised, personnel must notify their manager or HR before taking any steps.

3.8 Privacy

Personnel must respect and safeguard the privacy of personal information held by the Company regarding its clients, suppliers, Personnel and others. If Personnel have access to this information, they must ensure that it is collected, kept, disclosed, handled and used in a manner that complies with applicable privacy laws, any data protection laws that may apply and the Company Privacy Policies available on the Company's website and on the intranet.

3.9 Workplace behaviour and supply chains

The Company is committed to providing a workplace free of harassment, violence, bullying and discrimination. Personnel are expected to foster a respectful and inclusive work environment that adheres to the requirements of human rights law and related workplace legislation. The Company will not tolerate acts of discrimination based on age, race, colour, national or ethnic origin, disability, parental status, gender, sex, sexual orientation or any other ground of discrimination.

Personnel must act in accordance with the [Company's Workplace Behaviour and Respect policy](#).

The Company is also committed to ensuring that slavery and human trafficking are not occurring anywhere in the Company's business or supply chain, or by the Company's third-party business partners. Personnel are expected to adhere to the requirements of applicable modern slavery laws and related human rights law, and to communicate to, and uphold those requirements with, the Company's third-party business partners.

Personnel must act in accordance with the Company's [Modern slavery policy](#).

3.10 Protection and use of the Company's assets and property

Personnel must protect the Company's assets and property and ensure that the Company's assets and property are used only for the benefit of the Company's business. Personnel must report any suspected or actual theft or fraud to their Manager, HR or any other contact nominated by the Company.

Personnel must not use the Company's assets or property for personal purposes except in accordance with any Company policy or approved arrangement.

The obligation to protect Company assets includes the Company's proprietary information. Proprietary information includes intellectual property such as trade secrets and confidential information, patents, trademarks, designs and copyright, as well as business and marketing plans, engineering and manufacturing ideas, databases, records and any non-public financial data or reports. Unauthorised use or distribution of this information is prohibited and could also be illegal and result in civil or criminal penalties. The obligation to protect Company assets and proprietary information includes any assets or information (including confidential information) being held by the Company belonging to the Company's customers, clients, business partners and shareholders.

Personnel must return Company assets and property immediately upon request by the Company.

All expenses must be documented and reported in a timely manner, using the appropriate tools as directed by the Company.

3.11 Compliance with laws and regulations

The Company and its Personnel will comply with all applicable laws, rules and regulations in the jurisdictions in which the Company operates.

You must also comply with the technical and ethical requirements of any relevant regulatory or professional body. You must not breach, or omit to do something in breach of, any law or regulation or requirement.

All actual or potential breaches must be reported immediately to the Company Secretary or your manager.

Where local laws or regulations differ from this code, you must apply this code or local requirements, whichever sets the higher standard of behaviour.

Ignorance of the law or having a good intention does not excuse your obligation to comply. Personnel must participate in relevant compliance training programs offered by the Company.

If Personnel are uncertain about the interpretation of any applicable law or regulation or requirement, they must contact their Manager or HR.

3.12 Email and Internet Use

The Company provides personnel with access to email, internet and other computer-based tools to enable them to perform their duties and responsibilities for the Company. Use of these tools is subject to Company policies regarding acceptable use, as varied from time to time.

Personnel are hereby given written notification that emails, internet access and/or usage and computer usage will be monitored by systems administrators, IT staff and others, as nominated by the Company from time to time. The types of computer surveillance that may be carried out include, but are not limited to:

- (a) the monitoring and reading of emails sent, received and stored on the Company's computer network (including emails deleted from the Inbox);
- (b) the time, activity or application based monitoring of computer usage;
- (c) monitoring websites accessed by employees;
- (d) automated scanning of an employee's files to identify viruses or other malicious codes; and
- (e) logging individual keystrokes.

Personnel must act in accordance with the Company's [Information Technology Security Policy](#), [Acceptable Use of Information Technology Resources Policy](#), [Access Control Policy](#) and other related policies and documents.

3.13 Social Media

The Company expects its people to maintain a certain standard of behaviour when using social media for work or personal purposes. No employee is to engage in social media as a representative or on behalf of the Company without first obtaining the Company's written approval.

When engaging in social media activity (for private or work purposes), Personnel must:

- (a) do so in a professional manner, and act in the best interests of the Company at all times.
- (b) not engage in any social media activity that may bring the Company into disrepute or otherwise damage its interests;
- (c) not engage in social media activity that is discriminatory, defamatory, abusive, bullying or otherwise objectionable in content;
- (d) not make any commitment to any action or initiative on the Company's behalf without first obtaining the appropriate approvals;
- (e) comply with all of the Company's policies, and not breach any privacy legislation or policies;
- (f) not misrepresent the Company, or its customers, suppliers or Personnel; and
- (g) not disclose confidential information unless authorised to do so.

All Personnel must not communicate with the media in relation to any matters affecting the Company unless they have been authorised to do so by the Chief Executive Officer.

3.14 Responsibility to shareholders and the financial community

The Company is committed to providing value to its shareholders and recognising the legitimate interests of other stakeholders. The Company has policies regarding the timely provision of information to its shareholders and other stakeholders including posting information to its website. It has processes to ensure that the accounts and financial information it provides represent a true and fair view of the financial performance and position of the Company.

Personnel must fully cooperate with, and not make any false or misleading statement to, or conceal any relevant information from, the Company's auditors.

3.15 Insider trading

Insider trading laws prohibit a person in possession of material non-public information relating to a company from dealing in that company's securities. Insider trading is a serious offence.

The Company's [Trading Policy](#) is available on the Company's website and intranet. It provides guidance so that you do not deliberately or inadvertently breach the insider trading laws or the Company's policy.

3.16 Environmental responsibility

The Company considers both the environmental impacts and benefits of its decisions and business activities. The Company is committed to doing business in an environmentally responsible manner and identifying environmental risks that may arise out of its operations. Personnel must abide by all local laws and regulations and are expected to respect and care for the environment in which the Company operates.

Any Personnel who are aware of, or suspect, an action that is not environmentally responsible or in breach of the applicable laws and regulations, must contact the Leadership team.

3.17 Whistleblower protection

The Company is committed to the highest standards of conduct and ethical behaviour in all of our business activities and to promoting and supporting a culture of honest and ethical behaviour, corporate compliance and good corporate governance.

The Company encourages the reporting of any instances of suspected unethical, illegal, fraudulent or undesirable conduct involving the Company's businesses and provides protections and measures so that those persons who make a report may do so confidentially and without fear of intimidation, disadvantage or reprisal.

IPD Group has a [Whistleblower Policy](#) which is available on the Company's website and on the intranet.

4. Promoting and publishing this code

The Company and all its people leaders will promote this code across the organisation and provide training on the topics it covers.

The code is accessible by the company's website and intranet and communicated to all directors, employees and other persons as relevant. Key features will be published in the annual report or a link to the code on the Company's website provided.

5. Breach of this code

The highest standards of corporate conduct are critical to the Company's success and image. The values and policies in this code are not exhaustive. This code is designed to focus on particular values identified by the Company as central to its integrity.

Actions prohibited by this code involving directors or a Leadership team member must be reported to the Board. Actions prohibited by this code involving any other person must be reported to the Leadership team or the Chief Executive Officer.

After receiving a report of an alleged prohibited action, the Board or Leadership must consider the most appropriate policy and process that may apply to the alleged prohibited action and promptly take all appropriate actions necessary to investigate.

All Personnel are expected to cooperate in any internal investigation of an alleged prohibited action.

If a breach is found to have occurred, the Company will take such preventative or disciplinary action as it deems appropriate, including but not limited to termination of employment or engagement.

The Company does not tolerate acts of retaliation or victimisation, including demotion, dismissal, discipline, discrimination, harassment, suspension or threats, of or against any Personnel who makes a good faith report of known or suspected violations of this code.

6. Administration

6.1 Application of this code

If any part of this code is contrary to law or an industrial instrument, the law or industrial instrument will apply to the extent of inconsistency.

This code is subject to review by the Company and may be changed or revoked at any time.

6.2 Where to obtain further information

The Company has a dedicated person responsible for the administration of this code. At the date of adoption of this code, this is HR and the Board.

If personnel require further information or assistance or are uncertain about the application of this code or the law, please contact HR.

If any Personnel has a valid reason for not complying with this code, they should contact HR to consider whether to grant an exception.

6.3 Review of this code

This code will get reviewed from time to time and amended as required.