ESR GROUP LIMITED

CODE OF CONDUCT AND BUSINESS ETHICS

OWNER: GROUP COMPLIANCE

ESR Group Limited

Suite 2905-06, Two Exchange Square, 8 Connaught Place, Central, Hong Kong
T +852 2376 9600 | **www.esr.com**

Contents

1. INTRODUCTION

1.1 ESR Group Limited and its subsidiaries (collectively, "**ESR**" or the "**Group**") is firmly committed to conducting business in accordance with laws and regulations both in the letter and spirit (collectively, "**Laws**"), and ensuring that the rules and standards (collectively, "**Rules**") are complied by our directors, employees (full-time or part-time, permanently or temporarily employed), secondees, interns and officers (collectively, "**Employees**"). A violation of any Laws and Rules could have very serious consequences for ESR and for any Employees who violate the Code of Conduct and Business Ethics (the "**Code**") and such Employees will be subject to disciplinary action.

1.2 The Code is a general reference for use in all the countries in which ESR conducts its business operations. However, the Code does not describe all applicable Laws and Rules or give full details on any particular local policies. It does not constitute a legal advice or create a contract of employment.

1.3 ESR reserves the right to modify, revise, cancel or waive any policy, procedure or condition without notice and without revision of the Code. In addition, ESR may modify the provisions of the Code to adapt them to local Rules and conditions.

2. PURPOSE AND SCOPE

2.1 The Code sets out the ethical principles and standards of behaviour for ESR to abide regardless of the jurisdiction or legal entity of its business. It is established based on ESR's values (Excellence, Inclusion, Entrepreneurship and Sustainability) which guide our Employees of what to expect from themselves and each other when conducting business activities. The Group also expects any third parties including, but not limited to vendors, suppliers, contractors, agents, intermediaries, joint venture partners, representatives or consultants, or any persons with whom the Group has or may establish business relationships (collectively, the "**Third Parties**") to comply with the applicable provisions of the Code when performing such work or services on behalf of the Group.

2.2 The Group's subsidiaries and local offices shall adopt and implement the Code in adaptation to local regulatory requirements and/or in local languages, if necessary. Where there is a conflict between this Code and a local policy, the more restrictive provisions shall apply. If in doubt, please contact Group or Local Compliance for further guidance.

2.3 Employees are responsible for understanding and complying any legal and policy requirements that apply to their jobs and to report any suspected violation of this Code to Group or Local Compliance.

3. BUSINESS INTEGRITY AND ETHICS

3.1 All Employees must:

a) perform their duties with due care, diligence, honesty and fairness and ensure the avoidance of conflicts of interest or situation of undue influence at all times;

b) not disclose or divulge at any time, either during the course of employment with the Group or thereafter, any trade secret, material transactions or non-public information related to the Group's business;

c) not retain or duplicate for personal use any information, material or document that may come within their knowledge or possession during their employment with the Group;

d) abide by all applicable Laws, Rules and internal policies that apply to the business in countries where the Group operates; and

e) be committed to principles of good corporate governance which emphasise on transparency, accountability and independence.

3.2 The Board of Directors ("BOD") holds ultimate responsibility for overseeing business ethics across all operations and delegates authority to the Co-CEOs or another designated senior management on the said matter. While all Employees are accountable for the responsibilities above, senior management and business unit managers are also responsible for setting the 'tone from the top' and ensuring

Employees in their reporting lines adhere to this Code. They may be personally liable if they are aware that an act of illegal or unethical behaviour is happening or may happen, and do not take appropriate action to prevent it. The definition of senior management includes but is not limited to the BOD, C-suites, managing directors, head of offices, head of departments, senior management team of local entities and all business unit managers.

3.3 Acting ethically is not only morally correct, but also essential for conducting business responsibly. When making decisions or choosing a course of action, Employees should be guided by principles of integrity and fairness, not just by what is legally permissible.

4. CONFLICTS OF INTEREST

4.1 A conflict of interest ("**COI**") arises when an individual has a personal interest that conflicts with the interest of the Group, and such situation could affect the individual's ability to act objectively. A COI also arises in situations in which an individual is able to take advantage of his or her role for personal benefit, including the benefit of his or her family members (including spouse, parents or children) and associates. In relation to fund management, COI may arise between the investment manager or in a similar capacity providing investment management or related services ("**Advisers**"), their respective investors, and a fund or between multiple funds in respect of a particular investment. All Employees and Advisers must avoid COI that may arise between their personal dealings and duties and responsibilities in conducting the Group's business as well as in connection with the investment mandate of a fund. COI and potential COI which have been fully disclosed by Employees and formally permitted by the Group will not constitute violations of this Code.

4.2 Please refer to the Group Compliance's "**Conflicts of Interest Policy"** and ESR Fund Management & Capital's "**Conflicts of Interest Policy in relation to Fund Management & Capital"** for more details.

5. CORPORATE OPPORTUNITIES

5.1 Employees are prohibited from taking opportunities through the use of corporate property, information, or his/her position, without the consent of the senior

management, Group or Local Compliance. Employees should not take such opportunities for improper personal gain or directly/indirectly compete with the Group's business. Employees owe a duty to the Group to advance its legitimate interests when such an opportunity arises.

5.2 Employees have a duty to safeguard the Group's assets against theft, damage, wastage, or misuse and ensure their efficient use for legitimate business purpose. The Group's assets include financial assets, office equipment and intellectual property such as confidential business information and unpublished reports.

6. ANTI-COMPETITION, ANTI-TRUST, AND FAIR DEALING

6.1 All Employees should respect the rights of the Group's Third Parties (e.g., customers, suppliers, and competitors) for fair dealings. Employees should not take advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other illegal business practices.

6.2 Employees should ensure that activities and interactions with Third Parties reflect fair and proper business practices in compliance with the applicable Laws and Rules on anti-competition, anti-trust or fair dealing of the country which the Group operates, where Employees and Third Parties shall avoid any type of price collusion, cartel agreements or abuse of dominance, where applicable.

7. CONFIDENTIALITY

7.1 All Employees must maintain the confidentiality of proprietary information entrusted to them by the Group or its Third Parties (e.g., investors, business partners and customers). Disclosure of such information is only permitted when explicitly authorised, legally required, approved by senior management, or necessary for the performance of duties on behalf of the Group. Confidential information refers to any non-public information that Employees are required to safeguard from public disclosure. This information remains confidential regardless of whether it is explicitly marked as "confidential", "proprietary", or labeled in another way, and regardless of its form (i.e. whether spoken, written, illustrated, or electronically stored). Examples include, but are not limited to the Group's business plans, operations, policies, procedures, contracts, financial information and investments. This information must

be held in strictest confidence and must not be used for any purpose disclosed in whole or in part to Third Parties other than in the course of employment with the Group.

7.2 Employee in possession of confidential information should not under any circumstances:

a) use such information for his/her benefit and/or any Third Party's benefit;

b) use such information to influence any Third Party in dealing in any transaction;

c) communicate such information to any Third Party; and

d) disclose/use the Group's confidential information with third parties without proper authorisation.

7.3 Confidential information should be disseminated only to individuals who require it to perform their job responsibilities.

7.4 Employees must avoid discussing confidential information or reviewing confidential documents in public places (e.g. airports, planes, lifts and taxis).

7.5 The obligation of an Employee to preserve the confidentiality of information relating to the Group continues even after the employment has ended as outlined in the terms of the employment contract.

7.6 Upon the termination of employment, any information acquired by an Employee in the course of his/her service with the Group shall remain the property of the Group. The Employee shall return all documentation, digital memory/storage media and other materials (e.g. in a form capable of being returned) and shall not retain any copies or excerpts thereof or make use of such information for any purpose whatsoever.

7.7 Employees should adopt a clean desk policy as a best practice where applicable, such that:

a) all confidential information in hardcopy or electronic form should be secured in their work area at the end of the day and when they are expected to be away for an extended period;

b) any confidential information should be removed from the desk, stored away or locked in a drawer when the desk is unoccupied and at the end of the work day;

c) file cabinets containing confidential information should be kept closed and locked when not in use or when not attended;

d) keys used for access to confidential information should not be left at an unattended desk;

e) passwords should not be left written down in an accessible location; and

f) upon disposal, confidential documents should be shredded in official shredder bins.

7.8 Any loss or theft of office property (e.g. laptops and mobile devices) that contains confidential information must be reported immediately to the Human Resources and IT departments.

7.9 Employees must not send the Group's confidential information to their personal email accounts or upload it to personal cloud storage services.

7.10 For further information and guidance on confidentiality, the use of information and data, please refer to the Group Compliance's "**Employee Dealing and The Handling of Inside Information Policy**" and "**Privacy Policy"** on our website for more details.

8. ANTI-BRIBERY AND CORRUPTION

8.1 The Group takes a zero-tolerance approach towards bribery and corruption in any form and is committed to strictly abiding by all Laws and Rules that prohibit bribery and any other corrupt activities in countries where the Group operates. All Employees and Third Parties involved in the Group's business activities are strictly prohibited from offering, promising, giving, authorising, soliciting or accepting bribes in any form.

8.2 The purpose of business entertainment and gifts is to create goodwill and foster working relationships, and not to gain unfair advantage with Third Parties. No gift or entertainment should be offered, given, provided or accepted by any Employee unless (1) it is given as a basic matter of courtesy, kindness and respect (for example,

traditional festivals), (2) it is reasonable in value and where applicable, subject to pre-approval, and (3) it does not violate any Laws and Rules or applicable policies of the Third Parties.

8.3 Please refer to the Group Compliance's "**Anti-Bribery, Anti-Corruption and Handling of Gifts, Travel & Entertainment Policy**" for more details.

9. POLITICAL DONATIONS

9.1 The Group is committed to conducting business with integrity and does not make donations (monetary or otherwise) or lobbying expenses to political parties, political association and candidates and election agents in a parliamentary election or presidential election.

9.2 A political donation includes a gift or payment made to, or for the benefit of, a political party, an elected member of Parliament, a candidate or group of candidates, an employee of a Government department, or any person or entity who intends to use such a gift or payment to make a political donation themselves. A lobbying expense is any amount paid or incurred in an attempt to influence politics, including attempts to influence lawmakers, donations to candidates or campaigns, and money allocated towards political functions.

9.3 All gifts that are made for the benefit of a political party, an elected member, a candidate, or a person who intends to use the gift to make a political donation or lobbying expense are strictly prohibited. This includes any amount paid as an entry fee to political fundraising ventures or functions, such as political fundraising events or other briefing sessions hosted by a political party.

9.4 Employees are strictly prohibited to make political donations or lobbying expenses at any time on behalf of the Group or otherwise using funds of the Group. The Group shall under no circumstances have any sort of political contribution attributable to the entity.

9.5 Please refer to the Group Compliance's "**Anti-Bribery, Anti-Corruption and Handling of Gifts, Travel & Entertainment Policy**" for the definition of donation, Foreign Public Official and Government Official.

10. MONEY LAUNDERING, TERRORIST FINANCING & SANCTIONS

10.1 The Group adopts a risk-based approach in combating money laundering, terrorist financing ("**ML/TF**") and sanctions violations and is responsible for performing due diligence on any Third Party with whom we engage with by gathering their background information. Appropriate counterparty due diligence should be conducted to establish the true and full identity of each of the counterparty and its ultimate beneficial owner, ascertain the risk level and where applicable, determine the source of wealth and source of funds. Any knowledge or suspicion of ML/TF must be reported to the Money Laundering Reporting Officer / Group or Local Compliance. Failure to report suspicious transactions where a person has the requisite knowledge or suspicion, and tipping off to disclose to any other person any information that is likely to prejudice an investigation, could be deemed as criminal offences.

10.2 Please refer to the Group Compliance's "**Anti-Money Laundering, Counter-Terrorist Financing & Sanctions Policy**" for more details.

11. INSIDER DEALING

11.1 All Employees must be cautious if they are in the possession of material non-public price sensitive information / inside information (collectively, **"Inside Information"**) held by the Group, directors, or Employees in the ordinary course of business and strictly refrained from dealing in ESR Group Listed Securities[1] or making improper disclosure to the other parties. If an Employee acquires Inside Information or thinks he/she may have been passed with such information either inadvertently or otherwise, the Group or Local Compliance should be notified accordingly.

11.2 Please refer to the Group Compliance's **"Employee Dealing and The Handling of Inside Information Policy"** for more details.

[1] ESR Group Listed Securities include the following listed securities: (i) ESR-REIT (J91U.SI), (ii) Fortune REIT (0778.HK), (iii) ESR Kendall Square REIT (365550.KS), (iv) Prosperity REIT (0808.HK), (v) Suntec REIT (T82U.SI), (vi) ESR C-REIT (508078.SSE).

12. PROTECTION AND USE OF GROUP INFORMATION AND ASSETS

12.1 All Employees must protect the Group's information and assets, which shall be used for legitimate business purposes only. Disclosure of any confidential or proprietary information related to the Group to external parties is strictly prohibited unless prior authorisation has been obtained from senior management. In such cases, the external party must enter into a confidentiality agreement or an equivalent legally binding arrangement before any information is shared.

12.2 Confidential or proprietary information may include intellectual property such as personal data, counterparty information, trade secrets, copyrights, patent, domain names, design rights, databases, and unpublished financial data and reports. The unauthorised use or disclosure of this information constitutes a breach of company policy and may result in disciplinary action, up to and including termination of employment.

13. DATA PROTECTION

13.1 The personal data privacy policy sets out the general requirements relating to the management of personal data for the Group. The policy ensures the protection of personal data by maintaining its confidentiality and secure storage, while also helping to safeguard the organisation against data breaches.

13.2 Particular attention must be given to high-risk data**,** whose loss could result in significant contractual or legal liabilities, substantial harm to the Group's reputation, or considerable legal, financial, or operational consequences. In addition, many jurisdictions have specific Rules in place for the protection of personal data which can be defined as "any data relating directly or indirectly to a natural person, from which it is possible and practical to ascertain the identity of the individual from the said data".

13.3 In relation to personal data, restriction in cross-border data transfer and the mandatory breach notification to respective regulatory authority are the risks that may expose the Group to legal and compliance risks in countries where it operates. Advice should be obtained from the Group Human Resources, Group or Local Compliance if in doubt.

13.4 All Employees should protect the Group's data and comply with the applicable Rules. Please refer to the "**Privacy Policy"** on our website and Group IT's "**Information Security Policy**" for more details.

14. RECORD-KEEPING AND DISCLOSURES

14.1 The Group maintains accurate and timely recording and reporting of information to make responsible business decisions. All accounts must be documented and recorded accurately in a timely manner.

14.2 The Group's books, records, accounts and financial statements must be maintained in reasonable detail for statutory and audit trails purposes; and be in compliance with the applicable Rules for disclosure, reporting and record retention purposes.

14.3 Subject to local law requirements, all records should be retained for at least 6 years (or any minimum period as stipulated by local regulations).

15. MODERN SLAVERY

15.1 Modern slavery is defined as coercion, threats, or deception being used to exploit individuals and undermine or deprive them of their freedom. The Group takes a zero-tolerance approach towards modern slavery practices and is committed to taking appropriate action to prevent modern slavery and its humanitarian impact. The Group also does not tolerate any forced labour of any kind, including slave labour, prison labour, indentured labour, or bonded labour, including forced overtime hours.

15.2 Please refer to the Group Environmental, Social and Governance ("**ESG**")'s "**Human Rights Policy**" for more details.

16. DISCRIMINATION AND HARASSMENT

16.1 The Group is committed to providing equal opportunity of employment and takes a zero-tolerance approach towards discrimination. The Group also values mutual respect and maintains a workplace that is free of harassment, whether verbal, physical, visual, or sexual. If an Employee believes that he/she has been discriminated against

or have witnessed behaviour of discrimination, the Employee shall raise the matter to the Group Human Resources department.

16.2 Please refer to the Group "**Human Resources Policy**" for more details.

17. WORKPLACE SAFETY AND ENVIRONMENT

17.1 The Group is committed to providing a safe, healthy and drug-free workplace for all Employees working at its facilities and minimising impact of its operations on the environment. The Group places strong emphasis on conducting its business operations in accordance with industry best practices and maintains a well-governed development and management platform that strongly integrates ESG considerations.

17.2 Please refer to the Group "**Human Resources Policy**" and Group "**ESG Policy"** for more details.

18. RELATIONS WITH MEDIA

18.1 The Group is committed to provide clear, fair and balanced disclosure of pertinent information to directors, Employees, Third Parties and/or members of the public, where appropriate, in a timely and effective manner. The guiding principles are: (i) compliance; (ii) accuracy; (iii) timeliness; (iv) effectiveness; (v) fairness; and (vi) transparency. All external communication on behalf of the Group must be carried out solely by the designated Authorised Spokespersons of the respective entity.

18.2 Please refer to the Group "**Communications Policy**" for more details.

19. SOCIAL MEDIA

19.1 Employees should be aware and cautious in their use of social media which is a powerful tool in interacting with our stakeholders and ultimately affecting the Group's reputation. Social media posts include, but is not limited to, self-created content about ESR Group and work, sharing content from official ESR Group channels and interacting with content related to ESR Group on Third Party social media platforms.

19.2 Please refer to the Group Communications "**Social Media Policy**" for more details.

20. TRAINING AND ATTESTATION

20.1 The Group provides periodic training on the Code for new and existing Employees via the assigned e-learning course and other applicable training platforms to ensure that all Employees are aware of their personal obligations and responsibilities under this Code as well as the relevant legislation and guidelines.

20.2 Employees also receive communications that convey the 'tone from the top' on a regular basis and shall seek to comply with the form and substance of this Code and be aware of the implications and disciplinary actions as a result of non-compliance.

20.3 Employees are required to complete an attestation confirming their undertaking of and adherence to this Code, upon joining and on an annual basis.

20.4 Records of relevant training materials used, and attendance details of the participants will be maintained in the e-learning system and kept by Group Compliance.

21. REPORTING ILLEGAL OR UNETHICAL BEHAVIOUR

21.1 The Group is committed to maintaining high standards of business ethics and has adopted a whistleblowing policy and related reporting processes as essential elements of good corporate governance. For any violation of the Code, Employees should consult and report actual or potential illegal or unethical conduct to the Group or Local Compliance. Employees and external Third Parties who has business relationships with the Group can submit the report to the designated email address at whistleblowing@esr.com.

21.2 Please refer to the Group "**Whistleblowing Policy"** for more details, which is available for public access on ESR website (https://www.esr.com/whistleblowing-policy/).

22. **BREACH OF THE CODE AND DISCIPLINARY ACTION**

22.1 Employees who violate the principles in this Code may be subject to disciplinary action, including possible summary dismissal. It should be noted that the violations of this Code may also be subject to local Laws and Rules for possible criminal offence and prosecution.

Document Title	Code of Conduct and Business Ethics
Document Language	English
English Title	Code of Conduct and Business Ethics
Category	Group Policy
Policy Producing Function	Group Compliance
Document Author	Group Compliance
Document Approver	BOD
Portfolio Owner	Group Compliance
Original Issue Date	4 January 2017
Last Review Date	30 June 2025
Frequency of Review	Annually (or as required)
Version	1.9