ESKMUIR
GROUP

Eskmuir Asset Management Ltd
8 Queen Anne Street London W1G 9LD
Telephone: 020 7436 2339 Facsimile: 020 7436 2307

Governance Policy Statement

This Policy Statement sets out our approach in relation to corporate governance and compliance with legislation in the conduct of our business. Eskmuir is fully committed to the highest level of governance across our business and we look to achieve these commitments through continual review and improvement to our policies and processes, including the aim of requiring our third party contractors and consultants to similarly support our approach in their practices.

Our aim is to demonstrate continuous improvement through responsible business and property management practices, taking into account the various Stakeholder interests and requirements.

The key commitments of our policy are as follows:

- **Compliance**: Compliance ensures we work within the legal requirements applicable to the business and industry. If we do not comply, we are breaking the law. Eskmuir are required to comply with regulatory compliance including the Bribery Act 2010, the Money Laundering Regulations, and all other industry rules or legislative requirements. We seek that employees familiarise themselves with all these, and address these with managers.

- **Fraud**: Eskmuir will always seek to prosecute in instances of fraud and/or theft. We are determined to prevent, deter and detect all forms of fraud committed against and within it, whether by internal or external parties. All Eskmuir Directors and employees are responsible for conducting business in accordance with this policy, reporting any breaches they discover and promoting an anti-fraud culture. We will not accept any level of fraud and are committed to promoting honesty and integrity in all of our activities. We take the risk of fraud extremely seriously and will not tolerate any such wrongdoing. Any breach of the policy and related procedures will result in disciplinary action.

- **Data Protection and Privacy for Employees**: Eskmuir will hold and otherwise process data for the following principal purposes:
    - recruitment, promotion, training, redeployment and/or career development;
    - payroll data, including details of bank and building society accounts and salary transfers;
    - determination of certain benefits such as bonuses;
    - for contacting next of kin and arranging attention in connection with death, illness and injury whilst at work;
    - compliance with statutory and other requests from relevant public authorities such as the Inland Revenue and the Department for Work and Pensions;
    - disciplinary purposes arising from an employee's conduct or ability to perform job requirements;
    - undertaking reasonable monitoring of employees;
    - the provision of references following a request from our employees recent or potential employer; and
    - the provision of facilities and services in connection with employment.
    - It should be noted that this list of principal purposes is not intended to be exhaustive and that there may be other legitimate purposes for holding and otherwise processing data. Where the law so requires, employees will be notified of any additional proposed purposes.

- **Security**: Eskmuir will take reasonable measures to minimise the risk of fraud by protecting the security of both employee personal and Eskmuir's financial details, especially cheque books. Employees may use Company property remotely but it must be returned as soon as reasonably

practicable, and certainly before leaving employment at Eskmuir. Thefts and losses must be reported to a Director as soon as they become known.

- **Information Security**: The company's Information Security Policy sets out how to establish, implement, maintain and continuously improve its information security management system. Eskmuir will:
    - protect the integrity and reputation of our brand as trusted advisors to its clients and customers;
    - protect the confidentiality, integrity and availability of information assets;
    - comply with information security related contractual requirements of its clients;
    - protect the privacy of all stakeholders and particularly the personal information of its clients;
    - prevent unauthorised access to or use of its information and information processing facilities;
    - prevent unauthorised disclosure of its information;
    - manage any sharing of information with third parties, such as suppliers;
    - determine and maintain requirements for the continuity of information security within its business continuity arrangements.

- **Whistleblowing**: This policy makes it clear that anyone can raise a bribery concern or concern about possible fraud or corruption without fear of victimisation, subsequent discrimination or disadvantage. This policy is intended to encourage and enable individuals to raise serious concerns rather than overlooking a problem or publicising a concern externally. Initially, it would normally be expected that a concern would be raised with an immediate manager. This will depend on the seriousness or the sensitivity of the issues involved, and who is suspected of malpractice. If it is believed that an immediate manager is not the appropriate person to raise the concern with, then it should be escalated to someone in a senior position who would be able to provide the appropriate support, or discuss it with the Company Secretary.

The management team is committed to meeting these objectives and this is demonstrated by the systems, processes and practices adopted within Eskmuir.

This policy will be reviewed annually and will be communicated to all relevant stakeholders. It will be freely available upon request.

Date: May 2024