Waypoint Governance Policies

WAYPOINT ASSET MANAGEMENT

ANTI-BRIBERY POLICY AND RULES

Waypoint, which includes Waypoint's subsidiary and associate businesses have adopted the following policy to address Waypoint's obligations under the UK Bribery Act 2010.

The four main offences under the Bribery Act ("**the Act**") are:

- active bribery (i.e. giving, promising or offering an inducement to someone to do something that should otherwise be done in good faith or impartially or by a person in a position of trust);

- passive bribery (i.e. requesting, agreeing to receive or accepting a bribe);

- a specific offence of bribing a foreign public official ("FPO"), the definition for which includes persons who are not part of a government body such as persons who hold a legislative, administrative or judicial position of any kind, persons who exercise a public function or are officials of a public international organisation; and

- a strict liability offence which applies where a corporate or partnership fails to prevent "associated persons" performing services on their behalf (including employees, agents, intermediaries and introducers) from paying bribes. The only defence to this offence is to show that an organisation had in place "adequate procedures" to prevent such bribery.

Any suspicion that any of these offences has been or may be committed in connection with Waypoint's activities must be immediately reported to the Compliance Officer, who will consider the circumstances and notify the Serious Fraud Office as necessary.

PROCEDURES

Waypoint's directors are committed to ensuring that Waypoint meets its obligations under the Act.

Having considered the risks to the business, the Directors have determined that the key areas of relevant risk to Waypoint relate to gifts and inducements, introduction arrangements with third party marketers and the use of other agents. They have implemented the following procedures.

- Training is provided to staff so they understand the Act's provisions and area of focus and Waypoint's internal procedures to address the risks identified.

- The procedures described in other parts of the Waypoint Handbook for "Gifts, Benefits & Hospitality" should be followed in respect of all hospitality and gifts given and received. Care must be taken to ensure that business entertainment is not perceived as being over-extravagant, especially where FPOs are involved. Waypoint's internal procedures, as periodically updated, set out the levels at which entertainment may be considered to give rise to a conflict of interest and therefore require prior approval.
- The appointment of any introducer, agent, or intermediary must be approved in advance by the Board, who will determine the extent to which such appointment could bring Waypoint into contravention of the Act and who will further determine what controls should be put in place.

- Agreements with introducers, agents, and intermediaries should make reference to the Act and require the introducer, agent, or intermediary to confirm that they will not undertake any actions that would cause Waypoint to be in violation of the Act. Waypoint may request affirmation of compliance from relevant introducers, agent, or intermediary on an annual basis.

- No payments to third parties, other than bona fide payments to Waypoint's suppliers approved in the normal way by Waypoint's authorised signatories, may be made without advance approval in writing by the Compliance Officer and at least two directors following consideration of appropriateness under the Act. If there is any doubt as to the propriety of a payment, the matter must be referred to the Compliance Officer for guidance. In the unusual event of such a payment being made, following approval, a full record must be made including the payee, the reason for the payment, the person(s) approving the payment, any legal advice obtained and the reasons why the payment has been adjudged to be in compliance with the Act.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

COMPLAINTS HANDLING POLICY

Waypoint and its subsidiary and associate businesses ("Waypoint") have adopted the following policy in relation to complaints from customers and other relevant parties.

1. Policy

Waypoint requires the highest standards when executing its business and in treating its customers fairly. Waypoint therefore takes any complaint, however minor, extremely seriously. This policy sets out how complaints will be dealt with and, in relation to regulated business carried out by Waypoint, aims at conforming to FCA rules on complaint handling.

2. Guidelines

Waypoint will:

- acknowledge all complaints;
- investigate the complaint competently, diligently and impartially;
- assess fairly, consistently and promptly: what the complaint is about, whether it should be upheld and what action/redress should be taken;
- provide fairly and promptly: a clear assessment of the complaint, and an offer of redress or remedial action, if appropriate;
- ensure any offer of redress or remedial action that is accepted is settled promptly; and
- ensure a record of each individual complaint is made and, if it concerns a regulated activity, reported to the FCA.

3. Procedure

3.1. Acknowledgement

Regardless of whether a complaint is received during a telephone conversation or meeting, in a letter, email or other communication, Waypoint will record the concerns and pass the details to a director for investigation. The client will be notified within five business days, giving the name of the person who will handle the complaint.

All complaints should be passed to the Compliance Officer and notified to the directors.

Waypoint may, where it has reasonable grounds to be satisfied that another party may be solely or jointly responsible for the matter alleged in a complaint, promptly forward the complaint, or the relevant part of it, in writing to that other party.

Where this occurs Waypoint will inform the complainant promptly in a final response of why the complaint has been forwarded by it to the other respondent, and of the other respondent's contact details; and where jointly responsible for the fault alleged in the complaint, it complies with its own obligations in respect of that part of the complaint it has not forwarded.

Dealing with a forwarded complaint

If Waypoint receives a complaint that has been forwarded to it from another party, the complaint will be treated as if made directly to Waypoint and as if received by it when the forwarded complaint was originally received.

3.2. Investigation

The complaint will be investigated and an attempt made to resolve it as quickly as possible. Clients may be asked to provide additional information to assist in this process.

Within four weeks of making the complaint the client will receive either a final response or a response indicating when they may expect a final response.

Within eight weeks of making the complaint the client will receive either a final response or a letter explaining why Waypoint is not in a position to make a final response and when this can be expected. This letter will also inform of right to use the Financial Ombudsman Service, if applicable.

3.3. Resolution

Waypoint will always aim to resolve complaints within eight weeks and it should only take longer than this if it is necessary to request further information from the client or from a third party to establish all the facts.

The final response will set out the facts that have been established during the investigation and the redress to be offered, if any.

3.4. Reporting

Regulatory complaints from complainants, whether or not they are justified, will be recorded in the Complaints Register.

A separate record for ineligible complaints or complaints from ineligible complainants is maintained as these do not need to be reported to FCA.

4. Client Rights

An eligible complainant has a right to refer a complaint directly to the Financial Ombudsman Service but only after Waypoint has been given an opportunity to consider it and/or eight weeks have elapsed since the date of the complaint. An eligible complainant is defined by the FOS as:

- a private individual;
- a business which has group annual turnover of less than £1 million;
- a charity which has annual income of less than £1 million; or
- a trustee of a trust that has net assets of less than £1 million.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

DATA PROTECTION & CYBER SECURITY POLICY

Waypoint and its subsidiary and associate businesses ("Waypoint") have adopted the following policy in relation to the protection of data it holds or controls, including:

- all personal data of individuals Waypoint holds;
- the confidential data of Waypoint's clients;
- any such data Waypoint needs to share with its supply chain.

PERSONAL DATA

In relation to any personal data that it holds or controls, Waypoint will always:

- respect the privacy of all individuals whose personal information it holds or processes, irrespective of whether Waypoint is the controller of such data;
- treat all personal information under their control in accordance with applicable laws, including the General Data Protection Regulation of the European Union, the Data Protection Act 2018 and all UK domestic legislation relevant to data protection, including any amendments and enhancements thereto ("**Applicable Law**"); and
- not sell, rent, or loan any personal information in its possession to any third party.

Waypoint recognises that its data protection obligations under Applicable Law and the content of this data protection policy extend to all personal information in its possession, irrespective of whether the personal information was supplied at Waypoint's request, including in respect of:

- clients and investors, advisors and other individuals related to those clients;
- employees (and any persons who are provided as emergency contacts for them);
- service providers and contractors to Waypoint or its clients;
- tenants of clients' properties;
- visitors to Waypoint's website;
- persons making enquiries of Waypoint;
- persons making complaints about Waypoint, its clients or its service suppliers;
- business and professional contacts;
- job applicants and candidates.

Waypoint endorses and practices the principles of data protection contained in Applicable Law where data is required to be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- retained only for as long as necessary;
- processed in an appropriate manner to maintain security.

All personal information relating to any data subject given to an entity within Waypoint will be held with the utmost care and security in accordance with Applicable Law.

In particular, Waypoint will use personal information solely for the purpose for which it has been supplied.

Waypoint considers that personal information it holds on:

- clients and investors, advisors and other individuals related to those clients;

- employees;
- service providers and contractors to Waypoint or its clients; and
- tenants of clients' properties,

is held and processed for the execution of contracts and agreements between Waypoint and those parties and is therefore covered by the implied consent to the processing of such data under Applicable Law.

Waypoint holds and processes such data exclusively for this purpose, together with any other lawful purpose notified in privacy notices to individual data subjects.

Waypoint's policy with regard to:

- visitors to its website;
- persons making enquiries of Waypoint;
- persons making complaints about Waypoint, its clients or its service providers; and
- business and professional contacts;
- job applicants and candidates,

is set out in Waypoint's comprehensive data privacy notice contained on its website.

In accordance with Applicable Law, Waypoint will have in place privacy notices in relation to personal data controlled or processed by Waypoint. To the extent required by Applicable Law, these will be directly supplied by Waypoint or its managing agents, or made available (for example via Waypoint's website) to data subjects of Waypoint and its entities.

CLIENT INFORMATION

Waypoint recognises the particular sensitivity of personal information relating to its clients. In addition to the principles set out above applying to all personal data in Waypoint's possession, all personal information relating to a client or an underlying investor of a client that is supplied to an entity within the Waypoint group of companies will be retained by that entity in accordance with the contractual terms that govern that entity's appointment by the relevant client or investment vehicle and the laws and regulations, including Applicable Law and any data protection laws and regulations, of the relevant jurisdiction.

Personal information of a client, or its underlying investors, that is provided to a Waypoint entity will only be used by that entity to provide the client with the services that are to be provided to the client. Where considered necessary by the relevant entity in providing the services, such personal information may be provided to the other entities within Waypoint. Other than as required by law and applicable regulations or a Court order, a Waypoint entity will not provide any personal information of its clients to any entity outside Waypoint without the consent of the relevant client.

Waypoint recognises the rights of data subjects under Applicable Law, summarised below, and maintains appropriate measures in place to comply with these:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- rights in relation to automated decision making and profiling.

SUPPLY CHAIN SECURITY

Waypoint has appointed a number of third party sub-processors to supply services to Waypoint and its related parties, including its clients and employees. Waypoint requires all sub-processors it employs to treat personal data and confidential information with an equal degree of sensitivity and security.

Waypoint recognises the challenges raised by sharing data with its supply chain. Accordingly, insofar as they relate to its business, Waypoint will seek to follow the principles and guidance in relation to supply chain security promulgated by the National Cyber Security Centre. This relates to both personal and commercially confidential data Waypoint shares with third parties (together, referred to in this section as "Confidential Data"). Confidential Data includes data owned by Waypoint, its staff, the clients for whom Waypoint acts or other parties who have shared their data with Waypoint and/or its clients.

Waypoint's staff are required to adhere to Waypoint's detailed approach to supply chain security as set out in Waypoint's internal procedures, including the due diligence process for engaging with new suppliers.

ACCESS OF THIRD PARTIES TO WAYPOINT SYSTEMS

As a first principle, Waypoint will not provide external parties with access to any of its systems, unless such access is provided:

- to Waypoint's authorised IT consultants for development, maintenance and security purposes within contractual terms; or
- under controlled conditions (i.e. with Waypoint personnel present) and limited to a specifically agreed purpose; or
- for the purposes of data transfer (e.g. via a shared drive) authorised by a Waypoint director and limited to a specifically agreed purpose.

DATA PROCESSING AND SAFEGUARDING PROCEDURES

Waypoint uses standard office and business systems and applications commonly used throughout the UK and the European Economic Area ("**EEA**"), as well as specialist applications used within the real estate sector. The nature of modern data systems (e.g. the "Cloud") means that data processing and storage may not necessarily take place in the jurisdiction of the entity that provides services to the relevant client. It is possible that this will take place in countries with data protection legislation that differs from the UK and the EEA. The providers of the systems used by Waypoint indicate that personal information processed and stored outside the UK and EEA will be protected to the level required by the relevant contractual terms and the laws and regulations and any of the relevant jurisdiction.

Storage of personal information and record retention

Waypoint requires that all personal data relating to clients' investors, suppliers or key contact personnel (or any other personal information held) must be held in accordance with Applicable Law, in a secure format and only for as long as required.

Any of the above information that has been archived must be easily identifiable should Waypoint or its clients be requested to review a prior period.

Privacy related incidents

Any Waypoint team member discovering a privacy related incident, must inform a Director as soon as the information is available and ensure this incident is recorded. The Director will then inform the Board who, in the event of a data breach, will notify the appropriate supervisory authority within 72 hours of becoming aware of the incident.

Waypoint acknowledges that individuals have a right to claim compensation for damages caused by any infringement of Applicable Law by Waypoint.

Retention of data

Businesses must normally keep financial records for at least 6 years from the end of the last financial year they relate to, and the Board has adopted this as the standard retention period for all personal information held by Waypoint and its entities.

Any personal information contained in or required to back up such records must be kept securely during the standard retention period and any extension of it.

The need for the retention of personal data items must be reviewed following the sixth anniversary of the end date of the contract, agreement or circumstances giving rise to the control of processing of the personal data.

Records may need to be kept for longer periods if:

- they show a transaction that covers more than one of the company's accounting periods;
- the company has bought something that it expects to last more than 6 years, like equipment or machinery;
- the Board has confirmed that retention of the records is necessary for research or statistical purposes. This may apply, for example, to research information on investment properties that identifies individual tenants but is in a format whereby such personal information cannot readily be expunged.

Unless it is shown that there is an ongoing requirement to retain personal data items, those items must be referred to the Operations Manager for destruction, including any file or back-up copies.

The exception to this is Jersey data, which by law is required to be kept for at least 10 years.

Removal of data

If a client requests the removal of personal data from Waypoint's files, the request must be checked against the timelines above and the request authorised by a director.

Destruction of data

Waypoint's office has facilities for the disposal confidential hard copy personal client information. All such surplus hard copy information should be placed in the confidential shred bin. Any soft copy personal client information no longer required should be notified to the Operations Manager for disposal.

Data Security

All staff must ensure that all client data is appropriately secure at all times.

In particular, personal data:

- may not be transferred to or held on portable media (including USB sticks, floppy disks and mobile phones); or
- held on data files (including Word, Excel etc documents),

unless the relevant media or file is password-protected or the personal data is encrypted.

Hard copy documents containing personal data may not be taken outside Waypoint's offices without specific authorisation.

Appropriate measures must be taken to ensure the security or anonymity of all personal data transmitted outside Waypoint.

All staff must ensure that their visitors adhere to Waypoint's visitor policy at all times.

Staff personal files in hard copy are to be stored in a lockable facility, with keys to be held only by two individuals approved by the Board.

Automated decision making and profiling

Waypoint does not undertake any automated decision making (i.e. without human involvement) or profiling (i.e. automated processing to analyse or predict things about a data subject).

Marketing

Waypoint takes a responsible approach to marketing and will not issue client details, or details of related individuals, to any person outside Waypoint for marketing purposes.

Contact Information

For further information regarding how personal information is processed by Waypoint or to review personal information held by Waypoint, contact the Operations Manager.

Subject Data Requests

Subject access requests must be made to the Operations Manager in writing. For any such requests, the following guidelines apply:

- Requests can only be made about personal data held by the requestor. To make a request about someone else's data, they must provide their written, signed consent.
- Waypoint will require the requestor to establish identity. There is no prescribed manner for doing this but would typically include corroborating personal information or documentation such as a passport.
- Information will not be released over the telephone.
- Waypoint will provide, in a commonly-used format, a copy of the personal data it holds and the source of the data (where possible) as soon as is practicable and, in any case, within one month of the subject access request. If a data subject submits unreasonably repetitive requests, Waypoint has the right to charge a reasonable fee to cover administrative costs.

CYBER SECURITY - GENERAL

In addition to its specific obligation regarding personal data, Waypoint recognises the threats posed to itself, its clients and its workers by breaches of cyber security. Such issues may be caused by hacker attacks, viruses and system malfunctions, as well as human error. Waypoint recognises the financial and reputational damage that may arise from such security breaches.

Waypoint will therefore take all appropriate measures to ensure the security of all data it holds, whether that data relates to Waypoint, its clients or the persons it employs. Waypoint seeks to ensure data security through its operating environment, the systems and IT platforms it employs and the management procedures it adopts. Waypoint will apply this approach to all data in its possession, irrespective of whether data has been designated as confidential.

This policy therefore summarises the measures Waypoint adopts to minimise the risk of cyber security breaches, as well as the consequences should any breach occur.

This policy is to be applied in conjunction with the following Waypoint policies and procedures:

- Business Continuity Plan;
- Whistleblowing Policy;
- Security Incident Response Plan;
- IT Security; and
- Social Media Policy.

Scope

This policy applies to all persons who have access to systems and hardware operated by Waypoint, whether on a temporary or permanent basis. This includes remote workers and contractors, together with Waypoint's third-party advisers.

To maintain a consistent approach, Waypoint will treat all data held on its systems relating to clients, staff and contracting parties as confidential, unless expressly designated as non-confidential.

It is a fundamental obligation of all Waypoint staff to protect confidential data. Such data may not be communicated outside Waypoint, other than with the relevant party or its agents and advisers, without the relevant party's permission. Waypoint employees have a further obligation to report potential or actual data breaches to the Compliance Officer. All such reports will be dealt with confidentially under Waypoint's Whistleblowing Policy.

System security infrastructure

Waypoint will:

- use only IT platforms and systems that are reputed to possess robust security features;
- ensure that security updates for its IT systems are applied to systems and devices as soon as practicable after release;
- ensure that systems and data are protected by firewalls, anti-virus and access security facilities;
- ensure that access to its IT systems is granted only to authorised employees and that sensitive data is available to employees only on a "need to know" basis;
- provide IT security training to its employees;
- take swift and appropriate action to deal with reports of security weakness and actual breaches;
- investigate and learn from security breaches, taking action to prevent repetition;
- communicate regularly with its employees about developments in IT security issues.

Ultimate responsibility for the implementation of this policy lies with Waypoint's board of directors.

Passwords

A secure approach to systems access and passwords is a primary factor in ensuring data security. Waypoint team members are therefore required to follow internal rules on password selection and use.

Remote access

Each additional device used to access a system increases the risk of data security breach. For all remote devices used to access Waypoint's IT system, staff are required to:

- use two-way authentication DUO app when logging to office.com for access to SharePoint database and email.
- never download data from Waypoint systems onto non-approved devices;
- keep the number of remote devices used to access Waypoint systems to the minimum necessary;
- delete all data downloaded from Waypoint systems onto remote devices immediately it is no longer required for use;
- maintain password protection on all remote devices;

- maintain appropriate anti-virus software;
- ensure remote devices are not left unattended whilst Waypoint systems are accessed;
- install security updates as soon as practicable after they become available;
- access Waypoint systems only through secure networks.

Team members supplied with remote devices by Waypoint will be provided with security and access instructions when such devices are issued. Such instructions must be strictly adhered to, in particular for:

- data encryption set-up;
- password management;
- installation of anti-virus and anti-malware applications and update procedures.

Written instructions for accessing Waypoint systems must be kept secure and should never include user names and security passwords.

Staff must not access Waypoint systems using other parties' devices or systems unless these are certified as secure.

Electronic mail

Electronic mail is a significant source of cyber security breaches, being used to launch potential fraudulent scams as well as carrying malicious software. In view of this, staff are therefore required to:

- only use a secure email platform for sending emails containing sensitive/personal data
- check the names of message senders to ensure they are genuine – fraudsters often use email addresses very similar to legitimate contacts;
- not to open attachments unless they are adequately explained in the text of the accompanying email;
- be suspicious of emails offering free offers, prizes etc.

Any emails giving rise to suspicion must be referred to the Compliance Officer.

Data transfer

When transferring data, employees must:

- only use approved secure platforms
- apply appropriate security settings: restriction to edit, set expiry date, restrict access only to intended persons
- confirm that the data transfer is necessary and has been authorised by the subject party;
- ensure that data is not transferred using a publicly-accessible connection;
- confirm that any third party to whom data is transferred is authorised to receive it and has appropriate cyber security facilities, as set out in the section on Supply Chain Data Security below.

Dealing with cyber security incidents

Waypoint will deal with any cyber security incident in accordance with Waypoint's established Security Incident Response Plan (SIRP). Such incidents may also require the implementation of the steps set out in Waypoint's Business Continuity Plan.

Office and Operations

All employees are required to:

- adhere to internal rules on IT security;

- turn off computers at the end of the day;
- report missing or damaged IT equipment without delay;
- not download unauthorised software onto any equipment used for accessing Waypoint systems or use such equipment to access suspicious websites;
- adhere to the internal rules on the use of social media.

All staff are under a general obligation to report a perceived cyber security threat or weakness to the Compliance Officer as soon as possible.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

DIVERSITY, EQUITY & INCLUSION POLICY

Introduction and Policy Statement

The directors of Waypoint recognise that all individuals within its workforce, regardless of identity, background or circumstance, deserve the opportunity to develop their skills and talents to their full potential, work in a safe, supportive and inclusive environment, be fairly rewarded and recognised for their contribution and have a meaningful voice in contributing to the development of Waypoint's business as well as on matters that directly affect them. The directors of Waypoint commit to this Diversity, Equity & Inclusion policy in support of these aims.

Waypoint is committed to being an organisation that values everyone within it as an individual, recognising the benefits of a diverse workforce. In a similar vein, Waypoint is committed to generating an inclusive working environment, in which everyone feels able to participate and achieve their potential.

Waypoint will always meet the requirements of UK laws on equal opportunities and discrimination (such as on race, ethnicity, disability, colour, marital status or religion). However, Waypoint's policy on diversity, equity and inclusion seeks to go beyond these minimum requirements and recognises the value that can be added to its business through employee well-being and engagement.

Waypoint will apply the principles of this policy in its dealings with all persons it has a relationship with, including clients, professional contacts, property occupiers and members of the public.

The content of this policy is subject to review to reflect changing circumstances, such as changes in law.

Policy Framework

Waypoint will not tolerate behaviour within its business that treats any individual less favourably by virtue of their race, ethnicity, physical ability, neuro diversity, gender identity, sexual orientation, marital status, religion or socio-economic background. Waypoint will treat seriously all complaints of bullying, harassment (including sexual harassment), victimisation and discrimination whether by or affecting employees, customers, suppliers, visitors, the public and any others in the course of its activities.

Any such behaviour by a Waypoint employee will be dealt with under Waypoint's internal Disciplinary Procedure.

Further, Waypoint:

- acknowledges the benefits for the sustainability of its business of valuing the diversity of thoughts, ideas and ways of working that people from different backgrounds, experiences and identities bring to the organisation;
- recognises that individuals have different personal needs, values and beliefs and will seek to be consistently fair, but also flexible and inclusive, to support both individual and business needs;
- acknowledges the advantage of having a range of perspectives in decision-making and the workforce reflecting the organisation's customer base;
- commits to maintaining fair employment policies and practices, supportive of an inclusive working environment in which all employees feel that their contribution is valued and they are able to perform to their full potential, irrespective of their background, identity or circumstances;
- will be alert to and address the potential for "hiring bias" in job descriptions and advertisements;

- will be receptive to the concerns of individuals and monitor workplace behaviours to identify matters of concern and take appropriate action to address individual issues or entrenched attitudes that may be identified;
- will make appropriate interventions, including management and workforce training, in support of this policy;
- commits to maintaining an open culture based on dialogue, giving due consideration to employee's ideas and supplying appropriate action/feedback and developing supportive formal and informal communication channels;
- will ensure that its working practices are supportive of the objectives of this policy;
- will regularly review and evaluate progress with the effective of this policy, including monitoring key workforce data and consulting its workforce, and making appropriate changes as needed to achieve policy objectives.

Waypoint's staff are required to co-operate with efforts to ensure that the policy is implemented in full. This includes the supervision of Waypoint's agents, suppliers and contractors, whom Waypoint will always require to comply with this policy in relation to Waypoint's activities. Any member of staff who believes that they have been treated in contravention of this policy is encouraged to pursue the matter through the Grievance Procedure including, if necessary, making use of the Whistleblowing Procedure.

All Waypoint staff are encouraged to participate fully in the formal and informal communication forums established by Waypoint's directors, to share ideas and suggestions regarding the well-being and development of the business.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

EMPLOYEE WELL-BEING POLICY

Waypoint and its subsidiary and associate businesses have adopted the following policy in relation to the well-being of all who work in its businesses.

POLICY STATEMENT

The directors of Waypoint recognise the benefits of adopting a positive approach to the well-being of those working in its business, including:

- maximising employee morale;
- developing an increasingly inclusive culture and improved communication;
- reducing staff absence and turnover;
- maintaining good relations with its clients;
- the relationship between mental and physical health;
- ensuring that individuals and teams are mutually supportive and productive and can perform to the best of their ability.

Recognising the value that the business can derive from these benefits, Waypoint places considerable emphasis on the recognition of employee well-being issues and supportive interventions.

APPROACH

Waypoint takes a holistic approach to employee well-being, through a variety of measures, as set out below.

Physical and Mental Health

As stated in Waypoint's health and safety policy, all staff are required to place paramount emphasis on the health and safety of themselves, their colleagues and others present on premises and facilities under Waypoint's control. This includes site inspections and travelling between sites.

Waypoint carries out risk assessments on its premises and periodic checks on the safety of equipment used by its staff, including portable equipment. Waypoint encourages its staff to have regular eyesight checks in relation to working with visual display equipment.

Staff who are absent through sickness or disability are required not to return to work until they are fit to do so, including obtaining a fit-to-work certificate from their doctor if necessary. Waypoint's have in place a sick pay arrangement designed to support this approach.

Waypoint will consider reasonable arrangements flexible working hours or to enable staff to work out of the office home on a part or full-time basis if that is considered to be an appropriate measure to support an employee (for example, if it is difficult for an employee to use public transport at peak travel times).

Waypoint encourages staff to discuss issues relating to stress and mental health with their line manager or a director in confidence. Waypoint encourages its management to monitor early signs of stress and make appropriate adjustments.

Waypoint will support staff by enabling them to take reasonable time off for advisory or therapy appointments and will make reasonable adjustments in the working arrangements for individual employees and teams, to enable them to address stress and mental health issues.

Working Environment

In designing its office space, Waypoint will take account of ergonomic factors as well as the need to foster an open and supportive culture.

Waypoint recognises the need for line management to be both effective and supportive, with managers appropriately versed in fostering a mutually supportive environment. Waypoint's directors and managers will monitor staff absence rates and other trends, so as to inform the need for appropriate interventions.

Waypoint directors will take account of the well-being of the workforce in determining team structure, individual workloads and working hours. Job design will take account of factors such as quality of work, job satisfaction and work-lie balance.

Waypoint directors recognise the benefits of consulting staff on innovations and changes and actively promote the discussion of fresh ideas. Regular team meetings are organised, and informal gatherings supported in pursuit of this approach.

Waypoint encourages its employees to recognise the benefits of a healthy diet and exercise and the participation in team sporting events as well as our participation in programmes supporting charities related to our industry.

Waypoint provides a series of social events to foster relations and communication between team members.

Waypoint Values

Both in its operational approach and its formal policies, Waypoint is clear about its core values. At the core of Waypoint's values is its ethical approach to doing business and the maintenance of trust between Waypoint and its clients. This approach is reflected throughout the policies formally adopted by Waypoint. In furthering its core values, Waypoint's directors will take the lead in ensuring that:

- Waypoint staff treat each other with respect, valuing the diversity that those of different backgrounds bring to the workforce;
- their management style is supportive of Waypoint's employee well-being policy, including seeking advice as necessary;
- employees' voices are heard and have a genuine input in decision-making;
- individual staff members are provided with an appropriate career development framework, supported by performance appraisal, appropriate training, coaching and mentoring;
- members of staff recognise their own responsibility for looking after their well-being and are provided with appropriate support in doing so.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

MODERN SLAVERY AND CHILD LABOUR POLICY

Introduction and Policy Statement

This document comprises Waypoint's human trafficking and slavery statement for the purposes of the Modern Slavery Act 2015 (the "2015 Act"), together with Waypoint's policy towards the use of child labour.

The directors of Waypoint recognise the misery of human trafficking and slavery in the modern world and the dangerous and debilitating circumstances associated with child labour. Waypoint will take a zero-tolerance approach in this area. Accordingly, Waypoint will not trade or partner with any business or organisation that knowingly has any connection with such practices, however indirectly.

This policy should be read in conjunction with Waypoint's other corporate governance policies, particularly the Criminal Finances, Anti-Bribery and Anti-Money Laundering and Client Take-on policies.

It is our intention, with the cooperation of our clients, service suppliers and staff, to continually improve our approach in this important area.

Child Labour

We will adhere to the standards set out by the International Labour Organisation regarding the employment of children and young people. In particular:

(a) children must not be recruited before they have reached the age of completion of compulsory schooling, and in any case not before the age of 15; and
(b) those under 18 must not be required to perform hazardous duties.

Clients and Suppliers

We have reviewed our client base and have concluded that the likelihood that any of our clients has any connection to modern slavery and child labour to be very low. We will, however, disassociate ourselves from any client found to be knowingly connected to modern slavery practices.

We have similarly reviewed our supplier chain. Our suppliers comprise those connected to the business of investing in and managing property assets, such as property surveyors and agents, and business suppliers generally, such as IT systems providers and auditors. We have concluded that the risk of any of our suppliers being connected to modern slavery is also very low. Again, we will disassociate ourselves from any supplier found to be knowingly connected to modern slavery practices.

We expect our suppliers to join us in taking a zero-tolerance attitude in this area. To this end we will require that all new and renewed contracts for retained suppliers include a provision whereby the supplier undertakes that they and any subcontractors they employ on our business will comply with the 2015 Act and the International Labour Organisation standards on child labour and that Waypoint shall be entitled to terminate the contract should this obligation be breached.

Action

During the 12 months beginning with the date of this policy statement, we contacted all of our retained suppliers to seek their assurance that they comply with the wording and spirit of the 2015 Act. We also reviewed our other governance policies to assure ourselves that they support this policy statement.

Ongoing Approach & Review

Waypoint staff are required to co-operate with efforts to ensure that the policy is implemented in full, including the supervision of Waypoint's managing agents and contractors.

Following the initial adoption of this policy, we took action to ensure that our staff are aware of the importance of modern slavery, how it can pervade the society in which they live and work and how individual attitudes and actions can assist in exposing and dealing with it. We will periodically review the effectiveness of internal training and take further steps as necessary. The issue of modern slavery will be included in all induction training for new employees and the subject will be included in our periodic refresher programmes. All Waypoint staff are encouraged to participate fully in the formal and informal communication forums established by Waypoint's directors, to share ideas and suggestions regarding the well-being and development of the business. The directors will welcome the discussion of modern slavery issues within this framework.

We will review the progress we have made in promoting a zero-tolerance approach to modern slavery with our suppliers on an annual basis.

As with all other Waypoint governance policies, we will review the efficacy of this policy on an annual basis and update its terms as necessary.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 16/01/2024

WAYPOINT ASSET MANAGEMENT

RESPONSIBLE INVESTMENT AND STEWARDSHIP POLICY

1. Introduction

Waypoint Asset Management is a real estate asset manager and adviser that creates and executes innovative and bespoke investment strategies for clients. We advise on over £1bn of capital across established and alternative real estate sectors throughout the UK.

2. Purpose

Waypoint acknowledges that it has a duty to conduct its business at both a corporate, fund and property level in a sustainable and socially responsible manner. We have a tradition of investing and acting responsibly which has been with us from the beginning and continues to drive us forward.

Waypoint is a signatory of the United Nations Principles for Responsible Investment (UN PRI). As a business, we are committed to taking an informed and active approach to responsible investment by incorporating a thorough consideration of environmental, social and governance (ESG) factors. This commitment defines our overarching approach to responsible investment and management of assets whose stewardship is entrusted to us by our clients.

3. Responsible Investment and Guiding Principles

Waypoint defines responsible investment and stewardship as the integration of environmental, social and corporate governance (ESG) considerations into its investment, asset management processes and ownership practices in the belief that these factors can have an impact on financial performance.

We are proud to work with a diverse range of clients, some of whom are also signatories of the UN PRI. We believe a responsible and sustainable approach to investment and asset management will enable us to deliver long term positive value to our clients and stakeholders.

The six principles of the UN PRI form the foundation of Waypoint's responsible investment policy (RI Policy) which is based on environmental, social and governance criteria.

Environmental: commitment to managing environmental impacts in the most effective and responsible manner through fostering active management with our key consultants, appointed property teams and seeking continuously to improve our level of environmental performance.

Social: commitment to respecting diversity, equality and to the importance of the health, safety & wellbeing at our buildings for employees, occupiers, visitors and communities.

Governance: having robust governance is fundamental to ensure we identify and manage risks. We respect international best practices such as the Principles for Responsible Investment (PRI) and monitor compliance of the organisation with best practices/legislation in mind.

Although the UK Stewardship Code 2020 (the "Code") is not directly applicable to Waypoint, we consider that our policies and procedures reflect the principles set out in the Code and support compliance with the Code of those of our clients who are signatories to it.

Our responsible investment beliefs and core principles are embedded into our culture, asset management and investment process. We have developed a range of internal governance and risk management policies, requiring high standards of probity in the conduct of our business. The observance of these policies forms part of the employment terms of our staff members. It is this holistic approach that underpins our approach to responsible investment and stewardship.

Reflecting this, Waypoint has developed practical objectives which demonstrate how we integrate this policy into our overall business strategy and every day activities.

3.1 Environmental Objectives

- Implement conscientious management practices to measure and monitor all energy, carbon emissions, water and waste within our control.
- Collate data on flood risk, accessibility, and green transport credentials at both a property and fund level.
- Collate accurate data to identify baseline performance from which we can formulate clear and achievable targets including a roadmap towards carbon neutrality.
- Actively seek opportunities to use low carbon and renewable energy sources to reduce our carbon footprint.
- Commit to achieving net zero carbon in respect of Waypoint's Scope 1 workplace emissions by 2030.
- Commit to achieving net zero carbon emissions across our business activities and assets under management by 2050.
- Review our property portfolio regularly to identify sustainability measures to reduce operating expenses, reduce climate risk, increase efficiency, and improve the long-term value and resilience of our client's properties.

3.2 Social Objectives

- Promote and communicate the importance of ESG to our property managers, legal advisers, leasing agents and business partners through property management agreements, green leases and MoU.
- Provide training, resources and support to our colleagues and third-party property managers on ESG practices.
- Encourage and support suppliers with sustainable ESG practices and review their performance.
- Support the communities within which our assets serve.
- Seek opportunities to support local independent traders at our clients' properties.
- Create an environment that supports the health and well-being of our team, visitors, occupiers and communities.
- Monitor and improve employee engagement with regular employee satisfaction surveys.

3.3 Governance Objectives

- Manage and continuously review compliance with government requirements and any additional regulatory changes.
- Continue to provide and improve training to our team on governance topics.
- Demonstrate accountability and transparency to our investors of our ESG practices and performance through regular reporting and GRESB submissions.
- Waypoint's processes and operations are overseen by the Sustainability Committee and Waypoint's main board. Investment activities are overseen by an Investment Committee chaired by a Board member. These committees work together to ensure proper execution of investment strategies, consistent application of policies, compliance with procedures and local and regional regulatory requirements.
- Include all relevant ESG objectives within employee performance appraisals and personal development plans.

4. Implementation

Waypoint is committed to implementing this policy to ensure the assets that we acquire and manage are of the highest possible quality. We are integrating this policy into our investment decision making process, operations and across the asset lifecycle. From acquisition and in some cases development, through to operational use and sale we are following these steps to implement our responsible investment policy.

4.1 Positive and Negative Screening

- Waypoint and its associated funds will not invest in properties that are used for various unacceptable purposes or let to companies engaged in unacceptable business sectors.
- Where consistent with our fiduciary duty, we seek to give priority to occupiers who have a positive impact on the wider community, can demonstrate good governance and ethical business practices and have an established approach to diversity and inclusion in their workforce.

4.2 Transactions

- Undertake a risk assessment on potential acquisitions to include a review of EPCs, flood risk, energy, water, waste, ground contamination etc.
- Undertake due diligence on sellers, potential tenants and existing tenants (at rent review and lease renewal) in line with Waypoint and the client's policy at the time.
- As part of the acquisition due diligence investigate the potential to improve a property's environmental or social performance and budget for capital expenditure.
- Review the property's accessibility from a location and transport perspective.
- Review the property's health and safety aspects and areas for improvements.

4.3 Operations

- Where landlord controlled, measure and monitor the energy, water and waste consumed on a quarterly basis and establish targets for reduction and measuring improvement.
- Where responsibility for utilities is devolved, engage with tenants to measure and monitor the energy, water and waste consumed on an annual basis (where possible).
- All new leases granted should include green lease clauses to encourage landlord and tenant collaboration on ESG matters. At lease renewal seek to include green lease clauses.
- Incorporate ESG matters into property business plans at acquisition and ensure initiatives are reviewed on an annual basis.
- Ensure property managers and all suppliers maintain minimum ESG requirements and encourage best practice across the management of the portfolio.
- Encourage an active dialogue and co-operation between landlord, tenant and all stakeholders on ESG matters.
- Produce an Asset Sustainability Action Plan (ASAP) for each property to identify opportunities to improve the sustainability credentials and set a timetable for the implementation of feasible initiatives.

4.4 Developments and Refurbishments

- Identify opportunities to improve a property's environmental credentials as part of a refurbishment, where commercially viable. Where possible and practical to do so, track and assess the impact of energy improvements.
- Ensure compliance with MEES and ensure the team has a good understanding of current and future regulatory requirements.
- Ensure suppliers have robust procedures in place to manage ESG e.g. ISO 14001, Living Wage, Modern Slavery etc.
- Ensure environmental and social matters are considered throughout the refurbishment process including the health and safety of occupants, visitors and communities.

5. Scope

This policy is applicable to all of Waypoint's operations, employees and related persons. Those in scope should also have regard for this policy when appointing third-party suppliers and contractors as our aim is to ensure that we use our influence to deliver responsible investment for our clients, communities and environments in which we are active.

6. Governance

Responsibility for ESG across Waypoint ultimately rests with the Waypoint Board. This policy is reviewed at least annually by the Board.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 18/05/2023

WAYPOINT ASSET MANAGEMENT

POLITICAL CONTRIBUTIONS POLICY

Waypoint and its subsidiary and associate businesses ("Waypoint") have adopted the following policy in relation to contributions to political parties and causes.

1. Policy

Waypoint's overall policy is that it does not support any political parties or political causes.

2. Detail

In accordance with its policy statement, Waypoint will not:

- provide financial contributions to political parties or political causes;
- engage in or facilitate political lobbying;
- be associated with political campaigns or advertising;
- participate in fund-raising events for political campaigns;
- provide its employees with additional holidays or time off to enable them to take part in political events;
- enable its facilities to be used for political campaigning or fund-raising.

3. Support for Charities and Good Causes

In accordance with its commitments within its Environmental, Social and Governance agenda, Waypoint enthusiastically supports its staff in participating in voluntary fund raising and direct support events for appropriate charitable causes. Such causes will be scrutinised by Waypoint's Compliance Officer to ensure that the participation of Waypoint's staff does not contravene this policy.

4. Individual Rights

This policy will not infringe the ability of any member of Waypoint staff to participate in political causes within the law outside of working hours provided that they do not do so as a representative of Waypoint.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 18/07/2023

WAYPOINT ASSET MANAGEMENT

WAYPOINT ETHICAL CONDUCT POLICY

Waypoint is committed to acting ethically in all aspects of conducting its business. The fulfilment of this policy requires every Waypoint employee to act in an ethical way and accept personal responsibility for their actions in all of their dealings. The interests of Waypoint's clients are paramount and are placed above those of Waypoint and its individual employees.

In relation to this, Waypoint's staff are required to comply with the wording and spirit of Waypoint's adopted policies and procedural rules in the area of ethical conduct. These include Waypoint's policies on:

- Treating Customers Fairly
- Conflicts of Interest
- Personal Account Dealing
- Errors and Omissions
- Complaints Handling
- Anti-Money Laundering
- Anti-Bribery
- Criminal Finances
- Deal Allocation
- Responsible Investment
- Whistleblowing

These policies form part of the terms and conditions of employment of each member of staff. Any member of staff who is in doubt as to the appropriate course of action in any situation is required to raise the matter with Waypoint's Compliance Officer.

William A Heaney
Chief Operations Officer
Waypoint Asset Management Limited

Annual review date: 18/07/2023