



# | Waypoint Governance Policies

## WAYPOINT ASSET MANAGEMENT

### ANTI-FINANCIAL CRIME POLICY AND PROCEDURES

The directors of Waypoint Asset Management Limited, Waypoint Capital Limited and their subsidiary and associate businesses (“**Waypoint**”) have adopted the following policy and procedures to address its obligations in relation to financial crime, including (but not limited to) the following legislation:

- Proceeds of Crime Act 2002
- Serious Organised Crime and Police Act 2005
- UK Bribery Act 2010
- Money Laundering Regulations 2017
- Criminal Finances Act 2017
- Sanctions and Anti-Money Laundering Act 2018
- Economic Crime and Corporate Transparency Act 2023

#### GENERAL POLICY

We recognise the increasing prevalence of financial crime and the risks of financial crime within the property market. We are therefore committed to preventing financial crime through the policies and procedures set out below, which are based on the assessment of financial crime risks within each risk area.

In doing so, we will:

- operate a zero tolerance regime in relation to financial crime;
- communicate to our staff the importance of addressing financial crime and ensure that they undergo regular training in all key risk areas;
- ensure that appropriate resources are allocated to both the assessment of the risks of financial crime and all necessary compliance measures, including internal resourcing, training and communication;
- foster an open culture within our business that prioritises the enhancement of our reputation and our commitment to regulatory standards;
- encourage our staff to feel free to report any circumstances of concern either directly to management or confidentially through our Whistleblowing procedure;
- cooperate with enforcement authorities in the detection and suppression of financial crime.

This policy and the measures set out below form part of the terms of employment of Waypoint’s staff and failure to adhere to them is likely to be considered to be gross misconduct and may therefore result in the dismissal of those concerned. These requirements also form part of the terms of engagement of Waypoint’s contractors and we will consider the perpetration of a financial crime by a contractor to be a fundamental breach of trust. All such persons are required to adhere



to this policy and procedures and to provide all necessary assistance to Waypoint in all measures it takes in complying with its legal obligations.

## **PROCEDURES APPLYING ACROSS ALL FINANCIAL CRIME RISK AREAS**

1. Waypoint will adopt a risk-based approach to all financial crime risk areas, including them in its comprehensive risk register, which is reviewed regularly by the directors, and adopting procedures based on the objective assessment of the relevant risk. In doing so:
  - a) Waypoint's Compliance Officer will be primarily responsible for undertaking the assessment of financial crime risks faced by the business, including a focussed Financial Crime Risk Assessment, and its inclusion on Waypoint's comprehensive business risk framework, which assesses both likelihood and impact across risk areas;
  - b) The ongoing assessment of financial crime risks will include "horizon scanning" for new risk areas, in which all directors will assist the Compliance Officer;
  - c) The directors undertake that the Compliance Officer will always have direct access to the Board and such access will be immediate if deemed necessary by the Compliance Officer;
  - d) The risk framework will be reviewed by the Compliance Officer on a quarterly basis and presented to the directors at each quarterly Board meeting, including recommendations on risk mitigation for the Board's consideration and approval;
  - e) Recommended mitigation measures will be reasonable and proportional to Waypoint's exposure to the relevant financial crime risk area;
  - f) Policies and procedures across all financial crime areas, including the Financial Crime Risk Assessment, will be reviewed at least annually and will also be subject to immediate review to address any additional risk areas or regulatory changes that may emerge;
  - g) Whilst leaving no areas out of consideration, attention will focus on those areas and business processes identified as being of the greatest risk of financial crime;
  - h) Following their review of financial crime risks, the directors will ensure that the necessary resources are allocated to addressing the measures recommended as being reasonable and proportional to the risks identified
  - i) The Compliance Officer is also responsible for providing an annual MLRO report to the directors.
2. Waypoint staff are required to immediately report any suspicions that financial crime has taken place or is likely to take place to the Compliance Officer or, failing him/her, a director or confidentially through our Whistleblowing procedure. A template of the Waypoint Internal Suspicious Activity Report for use is available on the U: Staff Resource Hub.



3. Any such suspicion of financial crime shall be reported to the Board immediately and will be considered by the Board at the earliest opportunity, always having regard to the confidentiality requirements of the Whistleblowing Policy. Unless judged inappropriate in the particular circumstances, the Compliance Officer will always be involved in the Board's consideration of the matter and the Board will involve external advisors as appropriate.
4. Waypoint will in all cases request explanations from its counterparties and/or their advisors for unusual activity in transactions and will record such circumstances and explanations. Any such matter will be considered without delay by the Board and, in the absence of an appropriate explanation, the matter will be referred to relevant regulatory authorities, with whom Waypoint will cooperate.
5. The Board will adhere to its obligations for reporting suspicions of financial crime to relevant organisations, such as the Serious Fraud Office, the National Crime Agency and regulatory bodies and will cooperate with such authorities in dealing with the matter under consideration.
6. In the event that the Compliance Officer, or any other director or executive with anti-financial crime responsibilities, leaves the business or otherwise becomes unavailable for an extended period, the directors will ensure that adequate resource is put in place to enable that person's anti-financial crime responsibilities to be discharged.
7. The Board will ensure that appropriate records are kept of its consideration of its review of anti-financial crime risks and its consideration of any financial crime incidents that may arise, including reports and advice provided by consultants and dealings with relevant regulatory bodies, as well as the Board's decisions in all such matters.
8. The directors will ensure that sufficient resources are allocated to communication and training of staff in relation to all financial crime risks and mitigation measures;
9. The directors will monitor attendance on relevant internal training events, to ensure that all staff members attend, as well as reviewing the effectiveness of training events and communications, implementing improvements as required.
10. The involvement of a staff member will be treated as a serious disciplinary offence under Waypoint's Disciplinary Procedure, as set out in the Staff Handbook. A similar approach will be adopted in relation to any non-employee contractor.

Whilst the general policy and procedures set out above will apply to all aspects of financial crime, individual risk areas give rise to specific procedures, as set out below.

## **CRIMINAL FINANCES AND TAX EVASION**

We are committed to complying with the requirements of the Criminal Finances Act 2017 in reducing the opportunity for domestic and global tax evasion. We recognise that a business may be criminally liable for failing to prevent its staff or agents from committing such offences, even if the business was unaware of the tax evasion and including such evasion taking place overseas.



In addition to the processes set out above (PROCEDURES APPLYING ACROSS ALL FINANCIAL CRIME RISK AREAS), specific measures will be applied in relation to tax evasion risks. The offences under the Criminal Finances Act 2017 are:

- failure to prevent facilitation of UK tax evasion; and
- failure to prevent facilitation of foreign tax evasion

The ongoing measures listed below may be enhanced by additional measures recommended by the ongoing risk assessment set out above.

1. Recognising that financial services and property investment are viewed as high-risk areas for tax evasion activities, we will monitor and take full account of sector-focused guidance on risk mitigation.
2. Waypoint will request sight of the tax evasion prevention procedures of third-party advisors it recommends to its clients, and it will not recommend the services of any advisor that has failed to demonstrate reasonable prevention procedures.
3. The issue of domestic and global tax evasion and our approach to addressing this issue will be covered in our ongoing programme of staff compliance training.
4. The potential for tax evasion will be appropriately covered in Waypoint's Client Take-on process as well as the procedure for approving individual transactions, with special attention given to cross-border deals.
5. Agent and other third-party engagements arrangements will incorporate appropriate references to this policy, which will make explicit our obligation to report reasonable suspicions of tax evasion to the relevant authorities.
6. In developing new products and markets, due consideration will be given to any opportunity for tax evasion to which they may give rise, and appropriate risk reduction measures incorporated.

**Accordingly, all Waypoint staff are required to notify the Compliance Officer immediately if they suspect that a transaction in which Waypoint is involved may give rise to or facilitate tax evasion. This includes one-off transactions, such as asset purchases or sales, as well as ongoing transactions, such as rent payments or distributions to investors.**

## **ANTI-BRIBERY AND CORRUPTION**

In addition to the processes set out above (PROCEDURES APPLYING ACROSS ALL FINANCIAL CRIME RISK AREAS), specific measures will be applied in relation to bribery and corruption risks, as set out below.

The four main offences under the UK Bribery Act 2010 are as follows:

- 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
- the strict liability offence whereby an organisation fails to prevent its “associated person” 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.

These offences encompass activity taking place outside the UK, provided that the act or omission would have amounted to an offence had it occurred in the UK and the person who took some part in committing the offence has a close connection with the UK (for example British citizens and entities incorporated under UK law).

Having considered the risks to the business, the directors have determined that the key areas in which Waypoint could be at risk of bribery and corruption relate to gifts and inducements, introduction arrangements with third party marketers and the use of other agents. There could also be a risk in relation to construction, fit-out and repair and maintenance contracts, where the value of a contract or potential series of contracts, is high. Accordingly, Waypoint staff are required to adhere to the following procedures.

1. Attendance at relevant training events and updates, to develop a full understanding of bribery and corruption risks and Waypoint’s internal procedures to address the risks identified.
2. Adherence to the procedures described in the Staff Handbook for “Gifts, Benefits & Hospitality” in respect of all hospitality and gifts given or received, including the requirements for prior approval and reporting. Care must be taken to ensure that business entertainment is not perceived as being over-extravagant, especially where FPOs are involved.
3. Advance approval by the directors of the appointment of any introducer, agent, or intermediary, including determination of the extent to which such appointment could bring Waypoint into contravention of the Act and identification of any further controls needed.
4. Agreements with such counterparties 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.
5. No payments may be made to third parties, other than bona fide payments to Waypoint’s suppliers approved in the normal way by Waypoint’s authorised signatories, 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.

## PREVENTION OF FRAUD

Although Waypoint is not a “large organisation” directly covered by the Economic Crime & Corporate Transparency Act 2023, the directors have committed to adopt best practice measures in compliance with the Act’s provisions. Accordingly, Waypoint will maintain procedures proportionate to its exposure to the risk of fraud, including:

- commitment by its Board of directors
- risk assessment
- proportionate risk-based prevention procedures
- due diligence
- communication (including training)
- monitoring & review

The directors of Waypoint are committed to rejecting and taking all reasonable steps to mitigate against fraud, irrespective of any advantage that the perpetration of fraud may bring to the business. As well as recognising the criminal nature of fraud, the directors note that this commitment, and the anti-fraud processes arising from it, bring benefits to the business, including enhancement of Waypoint’s reputation and client confidence.

Whilst Waypoint’s designated Compliance Officer holds specific responsibilities in relation to assessment of financial crime risks and recommendation of mitigation measures, all directors acknowledge their shared obligations in this area.

In addition to the processes set out above (PROCEDURES APPLYING ACROSS ALL FINANCIAL CRIME RISK AREAS), specific measures will be applied in relation to Waypoint’s exposure to fraud risks, as set out below. The approach in assessing risks and developing mitigation procedures will take account of the “Fraud Triangle”, so as to:

- Reduce opportunities
- Reduce motives
- Reduce ability to rationalise

Risk Assessment will include:

- identifying “associated persons”, to determine the level of risk posed by various parties, including assessment by typology
- potential circumstances for fraud
- Adequacy of internal controls
- Adequacy of management oversight
- Whether reward targets / job security are too closely linked to measures which could be open to fraudulent activity
- Personal factors, including misalignment of goals and misunderstanding of corporate commitments
- Adequacy of Board anti-fraud commitment



Mitigation Measures will respond to recommendations arising from risk assessment. They will be proportionate to the identified risks, will seek to be practicable and effective. Ongoing measures are likely to include:

- Due diligence in staff/contractor recruitment and on-boarding
- Continual improvement of management oversight of operations/deals
- Regular review of contractors and sub-contractors
- Review of reward packages
- Monitoring staff well-being
- Review of the effectiveness of communication and training
- Monitoring changes in fraud risk faced by the business – e.g. as a result of changes in technology or introduction of new business streams

Waypoint Investment Management Limited (“WIML”) is subject to the WIML Compliance Manual, which contains provisions on prevention of fraud in relation to WIML’s activities, with which the directors and staff of WIML are required to comply.

## **ANTI-MONEY LAUNDERING & CLIENT TAKE-ON**

Anti-money laundering (“AML”) offences and compliance requirements are set out in a variety of legislation, referred to collectively as the “Regulations”. The content of this section contain the rules and procedures applied within Waypoint in compliance with the Regulations, under which it is a criminal offence for Waypoint not to have appropriate policies and procedures in place.

### **Guiding principles**

Under the Regulations, individual members of staff face criminal penalties if they are involved in money laundering or terrorist financing, or if they do not report their knowledge or suspicion of money laundering or terrorist financing where there are reasonable grounds for their knowing or suspecting such activity.

- It is of paramount importance that all staff discharge their duties in relation to the prevention of money laundering and combating the financing of terrorism in the clearest possible way and to the highest possible standards. During induction, all new staff are provided with a copy of the latest Anti-Money Laundering Personal Compliance Booklet for signature.
- It is vital that no investors participate in client funds, or investment management agreements put in place with new funds, if there is a risk that the fund, individual, or company concerned may have links to organised crime or terrorism.
- Staff must remain aware of the risk associated with money laundering and terrorist activities and of the legal requirements imposed on them.

Staff members must therefore maintain their awareness of their AML obligations and how to discharge them. Waypoint will provide regular training for every member of staff on AML and should you have any questions or be unclear on anything in relation to your duties you should contact the designated Money Laundering Reporting Officer (“MLRO”).



**Note that the due diligence and KYC checks described below must be carried out and recorded BEFORE a business relationship is entered into with the relevant party or parties.**

### **Risk-based approach**

As in other financial crime risk areas, Waypoint takes a risk-based approach to complying with the Regulations. Specifically within the property sector, the Regulations require estate agents, auctioneers and letting agents to register with HMRC and the sector is viewed by HMRC as being particularly vulnerable to financial crime. More generally, the Regulations require firms to:

- consult the register of Persons with Significant Control (“PSC Register”) maintained by Companies House, when performing anti-money laundering due diligence checks on prospective corporate client
- identify ultimate beneficial owners (“UBO’s”) for corporate clients
- consider whether the client or any UBO’s or PSC’s need to be checked as a potential Politically Exposed Person (“PEP”)
- carry out checks against the UK Government Sanctions List
- carry out Simplified, Standard or Enhanced Due Diligence checks as appropriate (see below).

### **Management responsibilities**

Oversight of the implementation of Waypoint’s anti money laundering policies and procedures, including the operation of the risk-based approach, is the responsibility of the MLRO under delegation from the board of directors. It is the responsibility of the MLRO to ensure that the appropriate monitoring processes across Waypoint are established and maintained.

Waypoint must ensure that risk management processes for managing money laundering and terrorist financing risks are kept under regular review. Accordingly, there is a need to monitor the environment within which Waypoint operates. Periodic assessment should therefore be made of activity in the marketplace.

Customers’ activities also change (without always notifying Waypoint) and the products/transactions attacked by prospective money launderers or terrorist financiers will also vary as perceptions of their relative vulnerability change. There is, however, a balance to be achieved between responding promptly to environmental changes and maintaining stable systems and procedures.

Waypoint will review its AML risk assessment at least annually and record the details of the review, including any updates agreed.

### **RISK ASSESSMENT AND IDENTIFICATION AND DUE DILIGENCE PROCEDURES**

A risk-based approach starts with the identification and assessment of the risk that has to be managed. Accordingly, Waypoint has identified the risks that must be managed, the assessment of these risks, and the corresponding CDD Identification requirements.



The discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the exposure to money laundering and terrorist financing must be undertaken on a customer-by-customer basis.

Waypoint has identified the following critical risk areas where the possibility of money laundering is an essential consideration:

- Client Risk – where the client onboarding process is key;
- Transaction Risk – comprising property or corporate acquisitions and disposals;
- Management Risk – involving asset management activity including (but not limited to) lettings, lease renewals, assignments and rent collection;
- Jurisdiction Risk - associated with the location of controlling individuals and sources/destinations of funds.

The procedures to be applied in each of these critical risk areas are set out in detail below.

### **Client Risk**

In considering whether to deal with any prospective client, the following should be considered:

- Is the client known to Waypoint personally (and, if so, for how long), an existing client or is it a new business relationship?
- Has the client been introduced by a third party?
- What is the nature of any third-party relationship and will it be ongoing?
- Have there been face to face meetings with the client and if not why?
- Is the client a private individual, limited company, trust or listed corporate entity?
- If a limited company, do we have full visibility including identity of the ultimate beneficial owner (“UBO”) and verification via Companies House records and documents (including the PSC Register)?
- Has the client or its representatives been evasive in supplying information?
- If no PSC is registered, why is this?
- Is the individual a Politically Exposed Person (PEP)?
- Is the person from a high risk or sanctioned jurisdiction (see High Risk Jurisdictions section)? If so, has their sources of wealth/funds been identified?

Consider critically the financial profile of the prospective client:

- What is the ultimate source of the client’s funds?
- Is the level of funds commensurate with the nature and status of the client?
- What is the nature of the client’s own business?
- Does the transaction involve complex structures?
- Is the client pressing to complete the transaction at pace, including cutting corners?

Take due account of the location of the prospective client and (if a corporate body) its principals:

- Where is the client based (UK, EU or other international location)?
- Is the client based in a high-risk jurisdiction or does it have links to a sanctioned country? (see High Risk Jurisdictions section, below)
- Does the transaction involve multiple jurisdictions?



- Is the client (or owning or controlling individual of a client company) a sanctioned person? (check against the UK Government Sanctions List: <https://search-uk-sanctions-list.service.gov.uk/>)

Verify identity:

- Have we obtained acceptable ID and proof of address for the client - ideally current passport and recent utility bill (see proof of identity checklist)?
- Is sufficient reliance or additional comfort available from other third parties such as the client's lawyers, accountants or bank?
- Has the client co-operated in the due diligence process or given rise to any concerns?

**NB: Prospective clients whose instructions involve regulated activities carried out by Waypoint Investment Management Limited, must always be subject to the checks set out in the WIML Compliance Manual.**

### Transaction Risk

For all property and corporate (i.e. share-based) transactions:

- Check that ultimate source of funds for approved Waypoint client has not changed;
- Establish that purchase is arms-length from an unconnected third party at or close to a justifiable market value;
- If the proposed transaction is at a significant variation to market value, request an explanation;
- Establish if KYC and CDD information is available from a regulated adviser or direct;
- Identify the UBO and PSC's;
- Identify the risk profile of the client and form a view on the appropriate level of due diligence (see below)
- Identify whether the transaction, including the source or destination of funds, involves a High Risk Jurisdiction (see High Risk Jurisdictions section, below).

Provided the above considerations have not raised any concerns, proceed to carry out the following internal control and record keeping processes:

- on all acquisitions complete AML section on Business Plans;
- on all disposals complete AML section on client recommendation form;
- flag any concerns direct to MLRO and always report any party deemed as high risk and subject to enhanced CDD.

For all lettings, lease renewals and property assignments Provided the above considerations have not raised any concerns, proceed to carry out the following internal control and record keeping processes:

- on all acquisitions complete AML section on Business Plans;
- on all disposals complete AML section on client recommendation form;
- flag any concerns direct to MLRO and always report any party deemed as high risk and subject to enhanced CDD.



For all lettings, lease renewals and property assignments You must ensure that each instruction to an agent includes written requirements for the agent to:

- warrant that they are appropriately registered with HMRC for Money Laundering Supervision;
- undertake to fully comply with the requirements of all relevant Money Laundering legislation, including carrying out and recording sanctions checks.

You must in any case:

- undertake Standard Due Diligence (or Enhanced Due Diligence, as appropriate) on all transactions with a rental value of £10,000 pcm or £100,000 per annum and above – refer to Due Diligence section below;
- request proof of identity and address from third party agents or lawyers (request direct if no third party involved);
- consult the MLRO in any situation requiring Enhanced Due Diligence – refer to Due Diligence section below.

## **Management Risk**

For dealing with client and tenant monies, such as rent collection and client monies:

- identify the AML protocols of any third party rent collection agents and verify that they are compliant;
- where required, obtain proof of third-party agent's registration with HMRC or other approved supervisory body;
- flag any changes to client payment accounts with the Finance Director and MLRO.

For new client money processes or variances in existing processes:

- complete AML section on all fund/client recommendation forms;
- save soft copy identification documents on the relevant file;
- flag any concerns direct to MLRO.

## **High Risk Jurisdictions**

A key requirement is to risk-assess the jurisdiction in which the client is based and/or operates. This involves consideration of countries:

- with a history of drug smuggling, corruption or money laundering
- identified by the Financial Action Task Force as high risk jurisdictions or jurisdictions under increased monitoring – see <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>
- subject to trade sanctions, especially those imposed by the Bank of England or OFAC
- scoring highly on Transparency International's Corruption Perceptions Index (<https://www.transparency.org/en/cpi>)

The UK Government's list of jurisdictions and persons considered high risk and subject to financial sanctions can be found at:



<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>

You must alert the MLRO immediately in the event that you consider the client falls within the High Risk category, so that appropriate steps can be taken.

## **DUE DILIGENCE**

Waypoint operates a risk-based approach to due diligence, whereby the standard applied is required to reflect the level of risk involved.

One of Simplified Due Diligence (“SDD”), Standard Due Diligence (“CDD”) or Enhanced Due Diligence (“EDD”) is always required. Your consideration of the risk areas set out above should guide which form of due diligence is appropriate. You should direct any queries as to the level of due diligence required to the Compliance Officer. Waypoint operated a Client Take-On Committee which considers and approves engagement with new clients.

However, the following internal control and record keeping processes are required in all cases.

- a. Waypoint Client Due Diligence Form to be completed for all new clients or funds
- b. Client Due Diligence Form to be approved and signed by both the MLRO and by a member of the Client Take-On Committee
- c. MLRO to retain a record of the approved MLRO with supporting verification documents or decide on next steps if red flags raised
- d. Standing instruction with Waypoint Accounts not to create a client account on relevant accounting and property management system until Client Due Diligence Form approved
- e. As a failsafe, no client engagement allowed until Client Due Diligence Form completed

The Client Due Diligence Form is set out at Appendix 1 and a template for use is available at U: Staff Resource Hub. If you have any questions around how it should be completed, please refer to the MLRO.

The terms of reference of the Client Take-On Committee are available at U: Staff Resource Hub.

**NB:** Transactions which appear to involve regulated activities carried out by Waypoint Investment Management Limited should be referred to the Compliance Officer or a WIML director, as they will be subject to enhanced due diligence and client take-on requirements.

### **Simplified Due Diligence (SDD)**

SDD is appropriate when a preliminary assessment indicates that a potential client or transaction poses a minimal risk of illegal activities. For Waypoint, such situations may involve:

- Low-Risk Customers, such as publicly listed companies or public institutions
- Low-Risk Transactions, that may be considered to have a minimal chance of being linked to financial crime.

The key steps for SDD are:



1. Confirm the client/transaction is low risk.
2. Gather basic identification details (see proof of identity checklist).
3. Verify information using reliable sources.
4. For corporate clients, form a basic understanding of ownership structure without in-depth verification unless risk changes.
5. Ongoing monitoring at a level reflecting the low risk.
6. Document the rationale for SDD, information collected, and verification steps.

### **Standard Due Diligence (CDD)**

CDD should reflect situations which raise a potential for risk, but which is unlikely to be realised. As noted in the Transaction Risk section, above, CDD should be undertaken as a minimum for value property transactions whose value exceeds a pre-determined threshold.

As a minimum CDD requires you to:

- identify the customer and verify their identity (see proof of identity checklist);
- For a corporate client, identify all UBO's and/or PSC's;
- Understand the nature of the client's business and the purpose of the proposed transaction;
- Determine the client's risk profile, including identifying the source of funds for the transaction;
- Monitor the client for any changes.

A UBO is any individual who ultimately owns or controls 25% or more of a business. This can be through intermediate entities and identification may require searching share registers, beneficial ownership registers and identifying voting rights or management structures. You should consult the MLRO if you need assistance with this.

PSC's should be identified on a company's PSC Register on the Companies House website.

For estate agency activities, the identify of each UBO or PSC identified must be verified and also checked against the UK Government Sanctions List. Waypoint's standard form of instruction to agents includes an undertaking by the agent to carry out this check and this requirement must be adhered to in all cases. If you become aware that this is not adhered to, consult the MLRO as soon as possible.

Consideration must also be given to whether such persons may be a PEP. If thought likely, then Enhanced Due Diligence (described below) must be undertaken.

The need for Enhanced Due Diligence must also be considered where Standard Due Diligence raises concerns. Such situations may include (though not limited to):

- no face-to-face contact with customer
- lack of clarity on source of funds or disposal destination of funds
- customer or funds come from a high-risk jurisdiction (see High Risk Jurisdictions section)
- deal arrangements or finance involves complex layering of corporate entities
- other red flags

### **Enhanced Due Diligence (EDD)**



- EDD must be carried out when there is considered to be a higher risk and increased opportunity of money laundering or terrorist financing, such as any of the circumstances listed above

In all such cases, you must report the situation to the MLRO. In any case, if you have any queries regarding the application of the above criteria in a particular case, also refer to the MLRO.

In such instances, consideration is to be given to EDD, including:

- establishing if an individual is a PEP;
- undertaking any adverse media checks;
- undertake a specialist risk search at either a personal or corporate level.

The identify of each UBO or PSC identified must be verified and also checked against the UK Government Sanctions List.

Consideration must also be given to whether such persons may be a PEP. If thought likely, then consult the MLRO for potential checking against a Politically Exposed Persons register.

## **REGULATED BUSINESS**

All regulated business within Waypoint is carried out by Waypoint Investment Management Limited (“WIML”). WIML is subject to the regulations of the Financial Conduct Authority, as an Appointed Representative of Langham Hall Fund Management LLP. These include enhanced anti-Money Laundering obligations, which are set out in the WIML Compliance Manual, to which all Authorised Persons of WIML and other Waypoint staff working on WIML’s business are subject. A copy of the WIML Compliance Manual is available at U: Staff Resource Hub/SH and Policy Suite. It may also be obtained from any WIML director or the Operations Manager.

**If the transaction under consideration appears to involve regulated activities, it should be referred immediately to a director of WIML or the Compliance Officer.**

# Appendix 1



<b>Waypoint Client Engagement Form</b>		
<b>To be completed and two copies printed for signature (one copy to client file, one copy to client Engagement File).</b>		
<b>No</b>	<b>Item</b>	<b>Response</b>
1	What is the name and address of the entity Waypoint will be dealing with?	
2	<p>If this is a legally registered entity, state type, jurisdiction of registration, registration number</p> <p>Has a copy of the incorporation document been supplied?</p> <p>(If jurisdiction is outside the EEA, refer to MLRO for guidance as to verification)</p> <p>Equivalent information to be supplied for government bodies, trusts etc.</p>	
3	Is the client acting for itself or a third party (if so, who)?	
4	If a third party could this be to avoid the third party having to undergo KYC assessment?	
5	What are the client's service requirements from Waypoint? Include the nature of the relationship with the client, as well as details of the clients business.	
6	Confirm that these activities do not comprise regulated activities under FSMA (refer any queries to the MLRO)	
7	What is the source of the clients' money, where it was generated from and where future revenue will be generated from?	
8	Provide contact details for the client's professional advisers and length of relationship.	



9	<p>Have you obtained proof on the client's letterhead that the person with whom you are dealing is authorised to act on behalf of the client in its dealings in which Waypoint is instructed?</p>	
10	<p>Has the client supplied a list of all persons authorised to act or sign on its behalf in its dealings in which Waypoint is instructed?</p>	
11	<p>If the client is a corporate body, has a list of all directors and beneficial owners (e.g. partners or shareholders) been supplied?</p> <p>Alternatively, if a publicly listed company, has proof of listing been supplied?</p>	
	<p>Have you seen original personal identity documents for the person acting on behalf of the client and for each person authorised to act or sign on the client's behalf in its dealings in which Waypoint is instructed?</p> <p>Two original official documents showing name and address, to include one of:</p> <p>Current signed passport. EEA member state identity card. Current EEA or UK photo card driving licence or a blue disabled driver's pass. Northern Ireland Voter's Card Home Office residence permit Shotgun or firearms certificate.</p>	



13	<p>Can the client be regarded as a <i>professional</i> client?</p> <p>For example, if the client is a:</p> <ul style="list-style-type: none"><li>government body</li><li>bank</li><li>dealer in investments or derivatives or conducts investment business on their own account</li><li>regulated firm or financial institution</li><li>company listed on a regulated market</li><li>pension fund or pension manager</li><li>collective investment scheme (UCITS)</li><li>credit institution</li><li>insurance company or broker</li><li>significant undertaking with:<ul style="list-style-type: none"><li>balance sheet &gt;€20m,</li><li>net turnover &gt;€40m or</li><li>net funds &gt;€2m</li></ul></li></ul>	
14	<p>Confirm that the client / client's jurisdiction or source of funds does not appear on HM Treasury sanction list.</p> <p>See: <a href="https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets">https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets</a></p>	
15	<p>Identify if any further reputational, adverse media or personal checks or searches are required.</p>	



## Appendix 2

### Waypoint Internal Suspicious Activity Report (SAR)

- Complete parts 1 - 4 of the form and submit to the MLRO [patrick@waypointam.co.uk](mailto:patrick@waypointam.co.uk), with subject heading SAR REPORT, together with any relevant supporting documents
- You should also arrange to discuss privately with the MLRO as soon as possible.
- State on the form if details are not known.
- If your report relates to a future transaction or a transaction currently in progress, speak to the MLRO immediately, in case he needs to raise a consent/Defence Against Money Laundering (DAML) suspicious activity report (SAR) with the National Crime Agency (NCA).
- The MLRO will assess the report and add any further relevant detail before submitting it the NCA through its portal.
- If for some reason you feel unable submit the form to the MLRO, you can refer to the Whistleblowing procedure or you can refer to the NCO website: <https://www.nationalcrimeagency.gov.uk/>

<b>Date</b>
<b>Transaction Name</b>
<b>Parties Involved in the Transaction</b> <i>Add as many boxes below as there are relevant parties</i>
<b>Party 1:</b>
Name
Address
Email
Phone
Additional Relevant Details
Involvement in the Transaction
<b>Party 2:</b>
Name
Address
Email
Phone
Additional Relevant Details
Involvement in the Transaction
<b>Reason for Suspicion</b> <i>NB:</i> <ul style="list-style-type: none"><li>• <i>Firstly, summarise your suspicion in a few sentences</i></li><li>• <i>Explain the type of transaction involved</i></li><li>• <i>If possible, explain events in chronological order and include all relevant dates</i></li><li>• <i>Explain how you became aware of the situation and what led you to being suspicious</i></li><li>• <i>Avoid acronyms and jargon</i></li><li>• <i>If you need to include technical details, give a simple explanation of these</i></li></ul>



- *Ensure your explanation answers the following questions: Who? What? Where? When? Why? How?*

**Supporting Documents**

*List any supporting documents you are submitting with the SAR*

**Reporter Information**

Name

Email

Phone

## Appendix 3

**WAYPOINT ASSET MANAGEMENT LIMITED (the “Company”)**

**CLIENT TAKE-ON COMMITTEE (the “Committee”)**

### PURPOSE

This document sets out the terms of reference and constitution of the Company’s Client Take-On Committee. The Committee is established by the directors of the Company as an integral part of the Waypoint group’s compliance process.

Waypoint’s Client Take-on process and the remit of the Committee applies to all entities within the Waypoint group.



## **CLIENT TAKE-ON COMMITTEE REMIT**

The remit of the Client Take-on Committee is to:

1. carry out the functions ascribed to the Committee under Waypoint's Know Your Customer ("KYC") and Customer Due Diligence ("CDD") rules as set out in the Waypoint Compliance Manual (and appended to these terms of reference);
2. contribute to Waypoint's compliance review regime by reviewing periodically the effectiveness of the KYC and CDD rules and, as necessary, making recommendations to the board of the Company.

## **MEMBERSHIP & QUORUM**

The membership of the Committee shall comprise a minimum of two directors of the Company, one of whom shall be the Company's director holding primary responsibility for regulatory compliance within the Waypoint group.

The Committee's initial membership shall be:

- Nick Gregory
- Patrick Smith (regulatory compliance member)

The regulatory compliance member must be present for all proceedings of the Committee. In the event that the other member of the Committee is unable to attend a meeting, he may nominate another director of the Company as a substitute.

The Committee shall be chaired by Nick Gregory.

The quorum for the Committee's meetings shall be two members of the Committee (to include the regulatory compliance member).

The prospective Client Relationship Director may not be a member of the Committee for its consideration of that client.

In the event that the Chairman is not available for a meeting the other members then present may choose one of their number to chair the meeting.

## **PROCEEDINGS**

Any director of the Company or of its subsidiaries and associate entities may notify the Committee's Chairman of the requirement for a meeting of the Committee. Ordinarily it is anticipated that the prospective Client Relationship Director of the relevant client.

On being notified of any such matter, the Committee's Chairman shall:

1. call a meeting of the Committee to consider the matter within a reasonable period of the matter coming to his attention;



2. ensure that copies of material for the Committee's consideration (including all comments or report from the Money Laundering Reporting Officer) are circulated to the members of the Committee in good time for them to be properly considered prior to and at the meeting;
3. consider whether it is appropriate to invite the Money Laundering Reporting Officer to relevant meeting of the Committee.

The Chairman of any meeting of the Committee shall ensure that:

- the Client Engagement Form and any supporting documentation is provided for the Committee's consideration;
- all relevant aspects are considered;
- the Committee's decisions are made on an objective basis, according to a proper interpretation of Waypoint's KYC and CDD rules;
- full consideration is given to any comments from the Money Laundering Reporting Officer;
- additional considerations raised by the regulatory compliance member shall be accorded appropriate weight;
- the Committee's decisions, and the reasons for them, are formally recorded;
- decisions of the Committee are relayed to all interested parties by appropriate means.

The Committee may invite any relevant person to attend a meeting of the Committee. Any question over the attendance of such person shall be decided by the Chairman.

The Chairman or a person appointed by the Chairman shall take minutes of the meeting, which the Chairman shall cause to be circulated within ten business days following the meeting.

The Chairman shall maintain a record of the Committee's proceedings and ensure that all relevant documents are placed on the Client Take-on Procedure folder on the Waypoint IT system.

Decisions of the Committee shall be by a simple majority of the members present. In the event of a tied decision, the Chairman shall have a casting vote.

Members may attend meetings of the Committee by electronic means.

**Nick Gregory**  
**Joint Managing Director**  
**Waypoint Asset Management Limited**

*Annual review date: 30/09/2025*

## **WAYPOINT ASSET MANAGEMENT**

### **COMPLAINTS HANDLING POLICY**

Waypoint Asset Management Limited and Waypoint Capital Limited together with their subsidiaries (collectively “Waypoint”) have adopted the following Policy in relation to complaints from customers and other relevant parties. This Policy must be read in conjunction with Waypoint’s Errors and Omissions Policy. In addition, this Policy has been drafted having regard to the rules and guidance of the relevant sections of the FCA Handbook.

#### **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. In relation to regulated business carried out by Waypoint, this Policy aims at conforming to the FCA rules on complaint handling.

#### **2. Guidelines**

Waypoint will:

- acknowledge all complaints;
- investigate the complaint competently, diligently and impartially;
- appropriately categorise the complaint having regard to Waypoint’s Errors and Omissions Policy.
- assess fairly, consistently and promptly: what the complaint is about, whether it should be upheld and what action/redress should be taken;
- ensure the complainant is kept informed of the progress of the measures being taken for the complaint’s resolution;
- 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;
- ensure a record of each individual complaint is made;
- if the complaint is in relation to regulated activities, reported to the FCA in accordance with regulatory requirements; and
- ensure that any complaint is only addressed after consideration has been given to the requirements and recommendations of Waypoint’s professional indemnity insurers.

#### **3. Procedure**

##### **3.1. Receipt and 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 by the Director within five business days, giving the name of the person who will handle the complaint.



All complaints must be notified to the Compliance Officer. Complaints will be notified to all Directors under Waypoint's standard reporting procedure, as outlined in Waypoint's Errors and Omissions Policy.

### **Third Party or Joint Responsibility**

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. Where Waypoint may be jointly responsible for the fault alleged in the complaint, Waypoint will comply with its own obligations in respect of that part of the complaint that has not been 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 the 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.

The client must receive prompt written acknowledgement that Waypoint has received the complaint and Waypoint is investigating the complaint.

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 the 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 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, taking into consideration:

- fair compensation for actual or potential financial loss;
- any reasonable costs incurred by the client; and
- the interest, at market rate, which may have accrued since the date on which the loss was suffered.



### **3.4. Investigating Root Causes**

Waypoint will assess whether, in handling complaints, it has identified any root causes which have been common to different types of complaints. In doing so, it will correct such root causes where reasonable and review whether these root causes may affect other services Waypoint offers.

### **3.5. Reporting**

Complaints related to regulated activities, whether or not they are justified, must be recorded in the Complaints Register. Assessment of whether complaints reflect breaches of regulatory conduct requirements will be carried out in line with Waypoint's Errors and Omissions Policy.

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.

**Nick Gregory**  
Joint Managing Director  
Waypoint Asset Management Limited

*Annual review date: 12/02/2026*

## WAYPOINT ASSET MANAGEMENT

### DATA PROTECTION & CYBER SECURITY POLICY

Waypoint and its subsidiary and associate businesses (together, “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;
- the systems and processes use within Waypoint.

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 consultants, together with Waypoint’s third-party suppliers.

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.

#### PERSONAL DATA

In relation to any personal data that it holds or controls, we 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.

This policy applies to all relevant data, whether held in electronic or hard copy format.

We recognise that our obligations under Applicable Law and this policy extend to all personal and confidential information in our possession, irrespective of whether the information was supplied at our request, including in respect of:

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



Our policy with regard to the above is set out in the data privacy notice contained on our website.

We endorse and practice 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 shared with us will be held with the utmost care and security in accordance with Applicable Law.

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

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.

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 the 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.

## **CLIENT INFORMATION**

We recognise the particular sensitivity of personal information relating to our clients. In addition to the principles set out above, all personal information relating to a client or an underlying investor of a client that is supplied to us will be retained in accordance with the contractual terms that govern our appointment .



Personal information of a client, or its underlying investors, that is supplied to us will only be used to provide the client with relevant contracted services. Where considered necessary, such personal information may be shared within Waypoint. Other than as required by law or a Court order, we will not provide any such information outside Waypoint without the consent of the relevant client.

## SUPPLY CHAIN SECURITY

Waypoint has appointed a number of third parties to supply services to Waypoint and its related parties. We require all such parties to treat personal data and confidential information with an equal degree of sensitivity and security.

We recognise the particular challenges raised by sharing data with its supply chain. Accordingly, insofar as they relate to our business, we will seek to follow the principles and guidance in relation to supply chain security promulgated by the National Cyber Security Centre: <https://www.ncsc.gov.uk/collection/supply-chain/guidance/12-principles>.

This relates to both personal and commercially confidential data we share with third parties, including data owned by Waypoint, its staff and clients or other parties who have shared their data with us and/or our clients. To understand the risks involved in sharing confidential data with its supply chain, we will:

**Identify** those items requiring protection, including their sensitivity and value and the impact that may arise from a data breach.

Identify **how** such data is shared with our supply chain, whether by shared systems, electronic transfer, physical access etc.

Identify **all those in the supply chain** with whom the data is shared and the security measures they have in place.

Understand the **risk profile** associated with the data and each party with whom it is shared, including that parties' vulnerability. In assessing the risk profile, we will refer to the National Cyber Security Centre criteria set out in the **Data/Supplier Security Profile** set out below.

Identify the **security measures and mitigations** suppliers have in place and their effectiveness, including those relating to sub-contractors, as referred to in the **Supplier Data Security Assessment** set out below. Where a supplier shares Waypoint's confidential data with its own supply chain, the assessment shall consider whether undertakings by the supplier are sufficient, or the exercise needs to be repeated for the supplier's own supply chain.

**Assess the effectiveness** of such measures and any shortfall against the standards required by Waypoint. As necessary, this will involve agreeing additional arrangements that meet Waypoint's requirements.

Put in place **control measures** to restrict or eliminate third-party access to data in the event that this becomes necessary, including procedures and key decision-makers for this process.

**Inform our staff** of the threats posed by cyber-security risks and their part in reducing such risks in relation to dealings with Waypoint's supply chain.



Ensuring that this policy is **embedded in our due diligence process** for engaging with new suppliers, including identifying which Waypoint personnel are responsible for confirming that the supplier's cyber security arrangements fulfil our requirements. This will include reflecting arrangements in contractual terms.

### **Access of Third Parties to Waypoint systems**

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

- to our 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. "Cloud" storage) 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 we used 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**

We require 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 the 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.

We acknowledge that individuals have a right to claim compensation for damages caused by any infringement of the Applicable Law.



## **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 we hold.

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;
- they relate to an investment that is expected to exceed 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 our files, the request must be checked against the timelines above and the request authorised by a Director.

## **Destruction of data**

Surplus hard copy information must 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 are obliged to 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.

## **Marketing**

Waypoint will not issue client details, or details of related individuals, to any person outside Waypoint for marketing purposes, without consent from those persons. Wherever applicable, Waypoint will require the recipient of confidential information to enter into a non-disclosure agreement.

## **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.
- We 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.
- In response to a subject access request, we will provide within one month, in a commonly-used format, a copy of the personal data it holds and the source of the data (where possible). If a data subject submits unreasonably repetitive requests, we reserve the right to charge a reasonable fee to cover administrative costs.

## **ARTIFICIAL INTELLIGENCE**

We recognise the increasing impact on cyber security of artificial intelligence applications. In the ongoing development of its Responsible Use of Artificial Intelligence Policy, Waypoint will take full account of the requirements of this Data Protection and Cyber Security Policy, the principles of which are regarded as paramount.

## **CYBER SECURITY - GENERAL**

We recognise the financial and reputational damage and personal impact that may arise from cyber security breaches and we have therefore identified cyber security as a key risk area within its risk management regime.

We will therefore take all appropriate measures to ensure the security of all data we hold and will seek to ensure data security through our operating environment, systems and IT platforms and



our management procedures. We will apply this approach to all data in our possession, irrespective of whether data has been designated as confidential.

Waypoint employees must 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. Team members are therefore required to:

- select "strong" passwords, at least 8 characters long with a mixture of numbers, upper and lower-case characters and symbols;
- avoid passwords that can be guessed at (such as a spouse's name/birthday);
- never supply system passwords to anyone else;
- be suspicious of anyone asking for a password – especially over the telephone (they may not be who they purport to be);
- avoid writing down passwords or giving a password to anyone else;
- change passwords immediately if there is any suspicion of unauthorised access to your work machine or Microsoft account.

### **Remote access**

Each additional device used to access a system increases the risk of data security breach. For all remote devices used to access our systems, 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;
- not to open attachments unless they are adequately explained in 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 Waypoint OneDrive for Business platform available on SharePoint
- 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**



We will deal with any cyber security incident in accordance with its established Security Incident Response Plan (SIRP) contained in Appendix 3. This includes actual data breaches or contamination as well as reported issues that are considered to have a material potential to give rise to a breach or contamination.

Such incidents may also require the implementation of the steps set out in our Business Continuity Plan, contained in the Staff Handbook.

The SIRP Team will co-opt external IT advisers as necessary to assist in dealing with the incident. The SIRP Team will also contact Cyber Security Insurance provider and consult legal advisers as necessary.

In the first instance action will be taken to contain and control the incident. This may involve:

- identifying the source of compromise, and the timeframe involved;
- reviewing the network to identify all compromised or affected systems;
- reviewing third party connections, virtual private networks and similar connectivity;
- changing passwords for authorised users and potentially disabling user accounts;
- universally denying access to compromised systems;
- physically isolating compromised components from the network;
- continual monitoring of systems for signs of intruder access.

In tandem with the above action, the nature and extent of the incident will be determined. Where there has been a breach of personal or commercial data, the following items are to be identified:

- the type of any personal information breached (personal identity information, bank details etc);
- method of breach (electronic, hard copy etc);
- extent and nature of client information breached.

Where systems are disrupted by virus or malware, information is to be gathered as to the extent of the disruption, the availability of back-up systems and data and the estimated workload and time to (a) disinfect systems; (b) restore systems and data and normal operating capacity. Where it is necessary to isolate equipment and replacements are required, timescales will need to take account of the availability of these and the need to install software.

Those clients, members of staff and others affected by any data breach will be consulted as early as possible in the process.

As soon as practicable, given the need to establish the extent of the incident and the response plan, the SIRP Team will draft an incident report to the Board. This will form the basis for internal communication and consultation with any affected clients and third parties, which shall take place as soon as possible, as well as any public statement deemed necessary.

The SIRP Team will make a record of events throughout the duration of the incident.

## **Office and Operations**

All team members must:



- adhere to the rules on IT security contained in the Staff Handbook;
- turn off their computers at the end of the day (it is in any case company policy for all PC's to automatically revert to "locked" mode after 10 minutes of inactivity, requiring a password to be entered);
- report missing or damaged IT equipment without delay to the Office Manager
- or Operations Manager (In such cases all the employee's passwords will be reset by Pensar engineers, and data erased as soon as possible);
- not download unauthorised software onto any equipment used for accessing Waypoint systems or use such equipment to access suspicious websites;
- adhere to the rules on the use of social media contained in the Staff Handbook.

All team members are under a general obligation to report a perceived cyber security threat or weakness to the Compliance Officer without delay.

### **Disciplinary action**

Employees causing security breaches may be subject to disciplinary action. Wilful breaches or those caused by gross negligence, are likely to be considered to be serious disciplinary offences and may result in dismissal.



## Appendix 1

### Data/Supplier Security Profile

<b>Tier</b>	<b>Security Profile</b>	<b>Description</b>	<b>Minimum security requirements</b>
1	LOW IMPACT from a supply chain cyber-attack or data breach	<ul style="list-style-type: none"> <li>No or limited reputational damage</li> <li>No or limited impact to business operations and/or processes</li> <li>No or minimal financial/legal consequences</li> </ul>	<ul style="list-style-type: none"> <li>Cyber Essentials scheme certification (or equivalent)</li> </ul>
2	MODERATE IMPACT from a supply chain cyber-attack or data breach	<ul style="list-style-type: none"> <li>Some reputational damage</li> <li>Some impact to business operations and/or processes</li> <li>Some financial/legal consequences</li> </ul>	<p>Tier 1 requirements plus:</p> <ul style="list-style-type: none"> <li>Defined and implemented data security policy, including incident management, employee responsibilities, access to data, user account and password management, including for mobile devices and removable media</li> <li>Defined Business Continuity/Disaster Recovery Policy</li> <li>Implement data security training, including provision for updates</li> <li>Pre-employment staff verification policy in place</li> <li>Record and maintain scope and configuration of information technology estate</li> <li>Policy for controlling information exchange via removable media and data transfer applications (e.g. One Drive for Business)</li> <li>Demonstrate security awareness and governance proportionate to size of organisation and value of data</li> </ul>
3	HIGH IMPACT from a supply chain cyber-attack	<ul style="list-style-type: none"> <li>High reputational damage</li> <li>High impact to business operations and/or processes</li> </ul>	<p>Tier 2 requirements plus:</p> <ul style="list-style-type: none"> <li>Compliance with Waypoint's data protection and cyber security policy</li> </ul>



	<i>or data breach</i>	<ul style="list-style-type: none"><li>• <i>High financial/legal consequences</i></li></ul>	<ul style="list-style-type: none"><li>• <i>Policy in place for granting access to Confidential Data</i></li><li>• <i>Policy in place for controlling remote access to networks and systems</i></li><li>• <i>Policy in place for secure storage of back-up copies of Confidential Data, if applicable</i></li><li>• <i>Monitoring and log management covering access to Confidential Data</i></li></ul>
--	-----------------------	--	--



## Appendix 2

### Supplier Data Security Assessment

*This form is to be completed in relation to all suppliers with whom Waypoint shares Confidential Data.*

<i>Supplier Name:</i>	
<i>Description of supplier service:</i>	
<i>Supplier Assessed by (Waypoint team member):</i>	
<i>Supplier Approved by (Waypoint Director):</i>	
<i>Date:</i>	
<i>Description of the Waypoint information the supplier is able to access and confirmation that this comprises Confidential Data:</i>	
<i>Potential Impact of Data Breach High/Moderate/Low (see Appendix 1):</i>	

#### Checklist

<b>Item</b>	<b>Y/N</b>	<b>Commentary</b>
<i>By what means does the supplier access Waypoint's Confidential Data?</i>		
<i>Confirm that the supplier does not have access to Waypoint's network.</i>		
<i>Is Waypoint's Confidential Data available to those in the supplier's own supply chain – if so, whom?</i>		
<i>Does the supplier's control environment extend to its own supply chain?</i>		
<i>Does the supplier have a named senior individual with responsibility for client data security?</i>		
<i>Are those with data security responsibilities suitably skilled and experienced?</i>		



<i>Are those dealing with Waypoint's data aware of their data security obligations?</i>		
<i>Are appropriate plans in place to deal with data incidents and are these adequate to maintain services to Waypoint?</i>		
<i>Do the contractual arrangements between Waypoint and the supplier state requirements for reporting and managing data incidents, including timescales and required actions?</i>		
<i>Is adequate protection in place for the supplier's IT networks, including physical servers and Cloud services?</i>		
<i>Does the supplier have control over all connections to its network?</i>		
<i>Does the supplier have effective controls in place to prevent authorised users accessing data outside their level of authority?</i>		
<i>Is there a robust process for identifying and authorising remote users?</i>		
<i>What security is applied to specific software applications used for Waypoint's data?</i>		
<i>If the supplier's users are allowed to use their own devices, what security controls are applied?</i>		
<i>Does the supplier's control environment reflect the Data/Supplier Security Profile set out above?</i>		



## Appendix 3

### IT Security Incident Response Plan

#### Scope

This IT Security Incident Response Plan is in respect of Waypoint Asset Management Ltd (“**Waypoint**”) and outlines the steps to follow on the occurrence of any incident that occurs by accident or deliberately that impacts our communications or information processing systems (“**Security Incident**”). A Security Incident means any incident that occurs by accident or deliberately that impacts our communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services which includes unauthorised access to, use, disclosure, modification, or destruction of data or services used by Waypoint.

#### Objective

The objective of this Plan is to ensure we act in an efficient and time effective manner should a Security Incident occur and to ensure that the business is able to continue to run and we are able to effectively service our clients and inform relevant parties of the attack and its impact with minimal disruption.

#### Roles and Responsibility

The Waypoint Security Incident Response Team (“**SIRT**”) is comprised of:

- Incident Response Lead Agnieszka Murach-Stepnowska
- Executive Officer / Risk Owner Mike Riley and Nick Gregory
- The Incident Response Technical Lead – **Pensar** Dean Ashbourne (Ph: **0333006 9550**)

If an incident should occur under the direction of the SIRT, each Director will be responsible for implementing this procedure for their team.

#### External Contacts

- **Police Action Fraud** – for reporting a criminal offence – **0300 123 2040**
- **ICO** – for reporting personal data breaches and security incidents/breaches – **0303 123 1113**

**Cyber Security Insurance** (Lockton Enterprise DataLock policy. Provider: Kennedys)

- **Breach event** – first contact Kennedys Law – **+44 203 137 8749** (24hr international hotline), email [DataLockclaims@kennedyslaw.com](mailto:DataLockclaims@kennedyslaw.com) and Lockton: [gctclaims@lockton.com](mailto:gctclaims@lockton.com)

See link below to Breach Protocol for further action required and other parties to notify:

<U:\11OFFICE\14Insurance\2024-2025CorporatecoversBreach Event Protocol for DataLock UK.pdf>

#### Procedure

#### Report



Security Incidents must be reported, without delay, to the Incident Response Lead or in their absence to another member of the Security Incident Response Team (**SIRT**). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.

In the event that a security incident or data breach is suspected to have occurred, the staff member should discuss their concerns with their line manager, who in turn may raise the issue with a member of the SIRT.

The Incident Response Technical Lead will identify the type of Security Incident and gather relevant diagnostic information.

### Investigate

After being notified of a security incident occurring, the SIRT will request that Pensar implement their security event and incident management policy and perform an initial investigation and determine the appropriate response to mitigate the risks associated with the incident.

The SIRT will also perform an initial investigation and determine the appropriate response which may result in the Security Incident Response Plan being initiated.

If the Security Incident Response Plan is initiated the SIRT will investigate the incident and initiate actions to mitigate the risks associated with the incident.

### Access to Compromised Systems

As soon as becoming aware of a security incident occurring:

- the affected computer should be disconnected from the network.
- The SIRT will notify Pensar so that they can undertake the necessary checks to ensure Waypoint's data has not been breached and quarantine any files necessary.
- If applicable, remove the HSBC & Natwest reader(s) from the machine and the Incident Response Lead will liaise with the banks so they can check there has been no unusual activity on the accounts that we operate.
- Pensar will preserve all logs and similar electronic evidence e.g. logs from the firewall, anti-virus tool, access control system, etc.
- The SIRT will maintain a log of all actions taken.
- Everyone should stay alert for further indications of compromise or suspicious activity in the environment.

### Inform

Once the SIRT has carried out their initial investigation of the security incident:

- The Incident Response Lead will liaise with the directors of Waypoint and the Chief Compliance Officer who will be responsible for informing all relevant parties, to include the Police, ICO and effected parties such as clients, investors and banks.

### Maintain Business Continuity

- The SIRT will engage with all teams to ensure that the business can continue to operate whilst the security incident is being investigated.

### Resolve



- The SIRT will liaise with Pensar and local law enforcement (if applicable) to ensure that appropriate incident investigation (which may include on-site forensic investigation at Waypoint offices) and gathering of evidence;
- The SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation from Pensar and Waypoint that the required controls and security measures are operational.
- The Incident Response Lead and Chief Compliance Officer will report the investigation findings and resolution of the security incident to the Board of Waypoint.

### Recovery

- The Incident Response Lead will authorise a return to normal operations once satisfactory resolution is confirmed and will confirm the same to the business.
- Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution.

### Review

The SIRT will complete a post-incident-review after each security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled in order to help identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Security Incident Response Plan and associated procedures.
- Updates to the IT Systems and Information Security Policy (contained in Appendix 1 of the Staff Handbook).
- Updates to technologies, security measures or controls.
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).

The SIRT Executive Officer/Risk Owner will ensure that the required updates and changes are adopted or implemented as necessary.

### **Specific Incident Response Types:**

#### Malware (or malicious code)

- Disconnect devices or isolate the network (user profiles/data) folders identified with malware from the network immediately.
- Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device. This will help you to understand how to remove it from the device.
- Once the malware has been removed a full system scan must be performed using the most up-to-date signatures available, to verify it has been removed from the device.
- If the malware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by the malware.



- Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

#### Unauthorised Wireless Access Points

- If unauthorised wireless access points are detected, or reported by staff, these must be recorded as a security incident.
- SIRT will investigate to identify the location of the unauthorised wireless access point/device.
- The SIRT will investigate as to whether or not the unauthorised wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented, and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
- All other unauthorised wireless access points/devices must be located, shutdown and removed.

#### Loss of Equipment

- The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the SIRT and local law enforcement. This includes losses/thefts outside of business hours and at weekends.
- If the device that is lost or stolen contained sensitive data and the device is not encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen.
- Where possible, Pensar will use available technology/software to lock down/disable lost or stolen mobile devices (e.g. smart phones, tablets, laptops, etc.). Evidence should be captured to confirm this was successfully completed.

#### Non-Compliance with IT Security Policy

This covers incidents resulting from deliberate or accidental actions that are in breach of the IT Systems and Information Security Policy and which put sensitive data at risk. This includes any systems or data misuse, unauthorised exposure of data to external parties and unauthorised changes to systems or data.

- The SIRT will engage with the relevant business area to establish an audit trail of events and actions and will determine who is involved in the policy violation and the extent of the violation.
- The SIRT will notify the directors of Waypoint of the incident.
- The SIRT will liaise with line managers to determine whether disciplinary action is needed.
- The SIRT will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example re-training of staff.

#### Training and Updates

The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members which will be included in the Firm's compliance training each year.



## **SUMMARY – Security breach checklist for users:**

- ✓ Make a note of any message on screen, don't click on any links!!
- ✓ Do not reply/forward any spam emails – take a screenshot
- ✓ Notify the office manager and/or IT help desk at Pensar as soon as you can
- ✓ Log out and switch off your PC, disconnect from the network
- ✓ Do not allow anyone to access the PC until it has been cleared for use
- ✓ Follow Waypoint's Security Incident Response plan (hard copy attached to SH located on admin shelf)

**Nick Gregory**  
**Joint Managing Director**  
**Waypoint Asset Management Limited**

*Annual review date: 21/08/2025*

## WAYPOINT ASSET MANAGEMENT

### ENVIRONMENTAL, SOCIAL & GOVERNANCE POLICY

Waypoint and its subsidiary and associate businesses have adopted the following policy to support Waypoint's sustainability ambitions and obligations.

#### **Policy Statement**

We have a responsibility to conduct our investment business in a socially responsible way and we recognise that our stakeholders are likely to have the same values. Taking account of this, we seek to deliver superior investment returns at the lowest possible cost to society and to the environment.

We support the six Principles for Responsible Investment promulgated by the United Nations and have incorporated ESG issues into our investment analysis and decision-making processes. We will use our influence as landlords to encourage our tenants and suppliers to do the same. As part of our commitment to these Principles, we participate in the UN PRI reporting programme and are a UN PRI Signatory

We also recognise that the built environment is a significant contributor to carbon emissions and that, as a manager of real estate investments, we have a duty to reduce the impact of those assets under our stewardship. This includes a commitment to quantifying our carbon emissions at corporate, fund and asset levels from which we can then set achievable reduction targets as part of a comprehensive net zero pathway.

All our staff are engaged in ESG issues in the conduct of their day to day business activities. Compliance is managed on a daily basis by a senior member of our staff as our dedicated ESG Officer. Progress with ESG issues is considered at all Board meetings.

As a business we believe it is important to be transparent in terms of both our adoption and delivery of sustainability led initiatives and in support of this are committed to the preparation and publication of a publicly available annual Sustainability Strategy & Report.

As Joint Managing Director, I am the owner of this policy, which will be kept under constant review and formally reviewed at least annually. I have overall responsibility for our compliance with this policy and hereby confirm that all the statements made herein are true.

#### **Nick Gregory**

Joint Managing Director

*"As institutional investors, we have a duty to act in the best long-term interests of our beneficiaries. In this fiduciary role, we believe that environmental, social, and corporate governance (ESG) issues can affect the performance of investment portfolios (to varying degrees across companies, sectors, regions, asset classes and through time).*



*We also recognise that applying these Principles may better align investors with broader objectives of society. Therefore, where consistent with our fiduciary responsibilities, we commit to the following:*

**Principle 1:** We will incorporate ESG issues into investment analysis and decision-making processes.

**Principle 2:** We will be active owners and incorporate ESG issues into our ownership policies and practices.

**Principle 3:** We will seek appropriate disclosure on ESG issues by the entities in which we invest.

**Principle 4:** We will promote acceptance and implementation of the Principles within the investment industry.

**Principle 5:** We will work together to enhance our effectiveness in implementing the Principles.

**Principle 6:** We will each report on our activities and progress towards implementing the Principles.

*We encourage other investors to adopt the Principles.”*

## **Environmental**

### **Guiding principles**

We recognise that our business activities have both direct and indirect impacts upon the environment and, hence, we have significant responsibilities towards the environment. We are committed to managing those environmental impacts in the most effective and responsible manner and seek continuously to improve our level of environmental performance.

Where consistent with our fiduciary responsibilities, we reduce the carbon footprint of assets coming under our direct control and encourage our joint venture partners and the managers of other funds in which we invest to do the same.

We measure the environmental performance of assets directly under management, by portfolio, with environmental improvement plans put in place for individual assets. We report progress to our investors at least annually or more often, when it is appropriate.

We engage specialist consultants to evaluate the sustainable characteristics of properties as part of our pre-acquisition due diligence, identifying risks to future financial performance and exploring opportunities to create additional value or to improve environmental performance. We also endeavour to assess the impact of new acquisitions on the overall environmental performance of the fund.

We will not ordinarily acquire buildings that fall short of our minimum standards unless we are able to demonstrate that affordable improvements can be made. Our minimum standard varies from fund to fund and with variations by sector and by region. We would not ordinarily acquire buildings, for example, with an Energy Performance Certificate rating lower than D without having an affordable plan in place to improve the rating during the period of the fund's ownership.



Where making a forward commitment to acquire new developments, we use our influence to encourage the developer and its contractors to consider sustainability-related issues in the design, construction and commissioning of buildings. We expect the environmental performance of new developments to exceed the minimum standards laid down by building regulations and planning policy. New commercial buildings should have a BREEAM rating of at least “Very Good”.

We expect all new buildings, both residential and non-domestic, to have Energy Performance Certificates rated at C or higher and that the design will incorporate enhanced insulation, advanced energy efficiency and a suitable range of water-saving features.

Aside from managing assets in an environmentally responsible manner, we see sustainability as both a threat and as an opportunity. There is a risk that the future value of some properties may be adversely affected by issues of sustainability. We have systems in place to enable us to measure, monitor and then manage these emerging risks as an integral part of our overall approach to risk management.

Conversely, we believe that some assets may experience a positive price correction as a result of the move towards a lower carbon economy and we are always looking for opportunities to create added value through the creation of more sustainable assets when considering asset allocation and stock selection.

Environmental sustainability is considered under these key headings:

- Financial performance
- CO<sub>2</sub> emissions
- Energy
- Accessibility
- Physical risks
- Water
- Waste
- Biodiversity
- Engagement
- Reporting

Some of these issues may have implications for the future financial performance of funds under management, and some relate to “best practice” and social responsibility. Our policy is intended to:

- Promote environmental protection and where possible aim for biodiversity net gain
- Prevent pollution
- Promote sustainable development
- Meet or exceed legal compliance and planning requirements
- Anticipate future policy impacts
- Establish risks from the physical impacts of climate change and develop mitigation strategies
- Minimise waste production while increasing recycling

While keeping our focus on maximising individual assets’ financial performance, we take account of our sustainability objectives by incorporating them into our business planning and reporting.



By integrating such issues into the investment appraisal process we aim to minimise downside risks and capitalise on opportunities for enhancing returns wherever possible.

Due to the ever-changing nature of sustainability practice we will continue to improve and update the relevant criteria that are used within the investment process.

## **Financial Performance**

We assess the likely implications of climate change policy on each individual asset and on the overall performance of each fund under our management.

In particular, we identify properties where there is a risk of losing income from existing tenants through migration to properties with better environmental qualities and quantify the potential impact of lower than average tenant retention rates, longer voids and higher costs on projected income returns.

We ensure that risks from sustainability-related issues are consistent with each fund's general appetite for risk and we devise strategies for reducing over-exposure to sustainability-related risks, during asset allocation and stock selection decisions and in the day to day management of funds.

We identify the cost of improvements that may be required, either to protect the future quality of an asset or as a result of statutory interventions and ensure that they are properly reflected in individual asset plans.

We monitor the emerging impact of sustainability-related issues on values and will amend performance projections and offers for future transactions in the light of hard evidence as it emerges.

We recognise that enhanced building standards and regulations may give rise to the potential for non-compliant assets to reduce in value or capability of occupation in the longer term. We will advise our investors of the risks and opportunities for such assets to enable them to make appropriate and timeous decisions.

## **Net Zero - CO<sub>2</sub> Emissions**

We recognise that greenhouse gases are a major contributor to climate change and controlling CO<sub>2</sub> emissions from properties under our management is therefore an essential part of our environmental strategy.

Where data is available, we calculate emissions from each property under our management and, where data is unavailable, make reasonable estimates as the basis for setting targets for future reductions using industry available benchmarks. We also seek to identify and allocate emissions within the recognized definitions of Scope 1,2 and 3.

When appropriate, we also calculate the "Carbon Intensity" (tonnes of CO<sub>2</sub> per £m invested and/or kgCO<sub>2</sub>e/m<sup>2</sup>) and, over time, we will seek to reduce the total volume of CO<sub>2</sub> emitted by properties under our management. This may be achieved through the adoption of more sustainable property management, through the physical improvement of selected assets or as a result of investing capital in better quality properties.



Current emissions are used as a basis against which measurable targets for year on year CO<sub>2</sub> emissions reductions at directly managed properties are set. We also establish the volume of emissions from each property and, when new properties are being brought under management, we assess the relative impact of each acquisition on overall emissions.

We have developed advanced net zero carbon pathways for all our individual fund mandates, as we believe these form a critical component of our wider asset management strategy and service to clients for a variety of reasons:

The focus has now shifted towards the delivery of carbon reduction targets with energy consumption and GHG emissions being the measurables by which our performance is quantified. We have adopted the Carbon Risk Real Estate Monitor (CRREM) modelling tool to assist us with measuring performance against net zero targets.

- Net zero pathways are required as a critical component of any strategy to align with recommendations of the Task Force on Climate-Related Financial Disclosures and also assist with increasing client led climate risk reporting.
- The incorporation and understanding of transition risk and asset stranding into the fund level strategies.

We take an equivalent approach to controlling and reducing carbon emissions arising from our corporate activities, where we have committed to achieving net zero emissions by 2050.

## **Net Zero - Energy**

Energy consumed is the most significant contributor to CO<sub>2</sub> emissions from the built environment and we are committed to conserving supplies, reducing consumption, and supporting green energy production and procurement whilst also reporting on our annual progress on a like for like basis.

- **Devolved**

At the majority of our buildings, we have no direct control over the way that energy is supplied and used by our tenants and have no ability to improve energy efficiency where responsibility for buildings has been devolved to our tenants. In these cases, we engage through our Managing Agents, with our tenants to encourage the more efficient use of energy and to promote energy efficiency improvements.

For selected buildings, we undertake a high level assessment of energy efficiency and identify ways in which energy efficiency can be improved. Where tenants are reliant on more carbon-intensive energy supplies, such as gas, we are exploring with them the practicalities of switching to electricity.

Where a Cost Benefit Analysis suggests that energy savings are proportionate to the costs, we invite tenants to undertake a more detailed assessment and give favourable consideration to applications for consent to alter.

We continue to monitor the effect on the built environment, including the property assets we are responsible for, of the national trend towards de-carbonisation of energy supply and the increasing reliance on the electricity grid.



- **Controlled**

We are directly responsible for the consumption of energy at a small number of multi-let buildings with common parts and shared services and have details of actual consumption.

We record consumption, year on year, and identify ways in which reductions can be made, setting measurable annual targets for each asset and across each portfolio as a whole.

We identify a range of energy efficiency improvements for each building under our direct control and determine whether the expenditure is justified in both environmental and financial terms.

We identify the most appropriate time to undertake improvements, having regard to existing tenancy structures and maximising opportunities to recover costs from tenants who stand to benefit significantly from lower building running costs.

In programming improvements, we also identify opportunities to reduce costs through making the relevant improvements at marginal additional cost during general refurbishment projects and during the routine repair and replacement of obsolete equipment.

Where there are opportunities to reduce energy consumption through the more efficient management of buildings or at little cost, appropriate instructions are given to the Managing Agents.

## **Accessibility**

We recognise that transport is a significant source of CO<sub>2</sub> emissions and that assets which are less accessible, based on the criteria set out below, may prove less attractive to occupiers and decline in value.

We examine the accessibility of all assets under our management and identify the extent of each fund's exposure to less accessible properties.

There is no common measure of accessibility but our analysis is based on three factors:

- **Distance from public transport.** Over-reliance on private transport generates higher emissions than properties which are well served by public transport. Offices, residential and retail properties which are more than one kilometre from suitable public transport may be considered relatively inaccessible.
- **Congestion.** Properties which rely on road transport (distribution facilities, retail warehouses, industrial properties) should be within easy reach of the national motorway network and accessible from a major trunk road without being ensnared in stationary traffic. Properties which are more than a 15-minute drive-time from the nearest motorway or major trunk road may be considered inaccessible.
- **Car parking.** The adequate provision of car parking can be a major contributor to the value of properties. Under-provision, displacing vehicles into neighbouring streets, will have a negative impact on the quality of the surrounding area. Over-provision may encourage the



unnecessary use of private transport. Buildings which differ +/- 20% from local standards may be considered inaccessible.

Where it is feasible and appropriate, we promote Green Transport Plans at assets under our management and ensure that buildings are equipped with appropriate facilities for cyclists and users of electric vehicles, including safe cycle storage facilities and electric vehicle charging points.

## **Physical Risks**

We recognise that some properties are at risk of flooding and that, in some locations, the risk of flooding may worsen over time as a result of climate change. In some cases, the risk is not reflected in current market values but expect that may change.

We identify which assets are at risk from flooding and forecast the extent to which values may be compromised. We ensure that the exposure of each fund as a whole is consistent with each fund's overall approach to risk.

We recognise that in some regions climate change also brings an increasing risk of overheating, requiring monitoring of the susceptibility of buildings to overheating and the adequacy of their ventilation systems.

On acquiring new assets, we have regard both to the impact of the issues set out above on the future performance of each asset and its impact on the overall exposure of the fund as a whole to those risks.

## **Water**

We recognise that water is a scarce commodity in some regions and that, over time, scarcity is likely to affect an increasing number of territories. We consider ourselves to be under an obligation to use all natural resources, including water, responsibly.

To this end, we promote the use of water-saving measures in areas of our buildings devolved to our tenants and, where we retain direct responsibility for the use of water, we explore ways in which it can be reduced at all our assets.

We instruct our Managing Agents to identify water saving measures that can be achieved at a reasonable cost.

We also evaluate the cost and likely return on more significant measures.

We also have regard to water saving opportunities during the regular repair, refurbishment and replacement of water-related services.

## **Waste**

We support the principle of "re-use, recycle, reduce" and its application to waste.

We encourage our tenants to recycle waste and to reduce waste sent to landfill sites and, subject to suitable space being available, will provide waste separation areas and recycling facilities at multi-let buildings under our direct control for the use of our tenants.



## **Engagement**

We recognise that the largest impact we can make on the environment is through influencing the behaviour of others – our staff, our agents, our contractors, our suppliers and our tenants.

We ensure all our employees are aware of our policy, objectives and targets and that relevant individuals have the knowledge and skills necessary to implement the strategy in their day-to-day roles. We provide appropriate training and knowledge dissemination to our staff.

Where we have responsibility for providing services to assets in our portfolio and engage the services of property managers or facilities managers, we ensure that our agents comply with our policy and adopt responsible management practices across the funds under our management.

Through our procurement policies and practices, we encourage our suppliers of goods and services to minimise the impact of their operations on the environment.

We engage with our tenants to encourage the sustainable management of areas under their direct control and in the way that common parts and shared services are used. We encourage tenants to make improvements to energy efficiency and, where appropriate, prepare high level “sustainable design guides” for tenants’ reference in preparing plans for fit outs and periodic refurbishments.

We identify tenants whose businesses are most influenced by sustainability-related issues and who have the most advanced Environmental Policies and explore ways in which tenants’ aspirations to reduce carbon emissions are consistent with the social and financial objectives of our funds.

## **Development**

We do not undertake direct development but may, from time to time, agree to forward fund development projects.

Where making a forward commitment to acquire new developments, we use our influence to encourage the developer and its contractors to consider sustainability-related issues in the design, construction and commissioning of buildings. We expect the environmental performance of new developments to meet and, where appropriate, to exceed the minimum standards laid down by building regulations and planning policy.

Commercial buildings should have a BREEAM rating of at least “Very Good”.

We expect all new buildings, both residential and non-domestic, to have Energy Performance Certificates rated at C or higher and that the design will incorporate enhanced insulation, advanced energy efficiency and a suitable range of water-saving features.

We encourage developers to use durable materials and, where appropriate, to ensure that adaptability, both within use and across uses, is incorporated into new building design.

We also encourage developers to re-use or to recycle materials when existing buildings are demolished and to re-use recycled materials during new construction.



Some retail properties sit beneath offices, many of which are of poor quality and economically obsolete. When it is viable, we will seek opportunities to convert this space into residential accommodation and, when appropriate, may create affordable housing for local residents. Compliance with current buildings regulations will be our minimum standard, although we will endeavour to exceed this minimum standard whenever it is commercially viable.

## **Social**

We recognise that our business activities have both direct and indirect impacts upon society and that we have a responsibility to minimise any negative impacts and, where it is consistent with our fiduciary responsibilities, to seek opportunities to make a positive impact.

The Local Retail Fund (where Waypoint Asset Management is appointed asset manager) is designed to provide local amenities for the residents of the locations in which we have invested. Both the Waypoint Government Income Fund and the funds managed by Waypoint Health Property Limited (“WHPL”) provide accommodation for public sector services, allowing organisations to use their capital for reinvestment in government, health and community services that might otherwise be tied up in property.

### **Negative Screening**

We will not invest in properties that are used for various unacceptable purposes or let to companies engaged in unacceptable business sectors. The list of unacceptable uses is kept under constant review and, at present, includes the following:

- Adult entertainment
- Manufacture of tobacco products
- Animal testing for non-medical products
- Production of animal fur
- Manufacture and sale of controversial weapons

### **Positive Screening**

When properties become vacant and need to be re-let, our first priority is to achieve the best rent available from the most appropriate tenant in order to satisfy our fiduciary responsibility to maximise income and capital returns from our investment. We do, however, recognise that some potential tenants will have a more positive impact on the local community and the local economy than others.

Where it is consistent with our fiduciary duty, we give priority to potential tenants who:

- Employ the greatest number of local staff
- Provide goods and services primarily to the local community
- Can demonstrate good governance and ethical business practices
- Have an established approach to diversity and inclusion in their workforce

Subject to competitive offers being received, preference will be given to public sector organisations and to healthcare and educational users.

### **Health, Safety and Well-Being**



We ensure that appropriate Health & Safety regimes are in place at all buildings under our direct control and encourage our tenants to do the same. Compliance with appropriate legislation and regulations is considered to be a minimum standard and, through our external property managers, will ensure that Health & Safety issues are kept under constant review and subject to quarterly review at our main board meetings.

We also recognise the benefits of adopting a positive approach to the well-being of those working in our business, including:

- maximising employee morale;
- developing an increasingly inclusive culture and improved communication;
- reducing staff absence and turnover;
- maintaining good relations with its clients;
- ensuring that individuals and teams are mutually supportive and productive and can perform to the best of their ability
- providing employees with opportunities to enhance their physical and mental well-being while contributing positively to social value through the Waypoint Social Responsibility and Employee Welfare committee initiatives

Further details of our approach to these issues are set out in our corporate Health & Safety policy and our Employee Well-Being policy.

## **Employment**

### **Compensation**

The Remuneration Committee reviews salaries, bonuses and other compensation on an annual basis. Members include the joint Managing Directors, who consult with the Board members and line managers as appropriate. A number of financial factors are taken into account, including individual performance, and group and unit performance. Non-financial factors taken into consideration include compliance with group policies including Environmental, Social and Governance matters. Particular performance and reward criteria apply to those employees whose roles include a significant proportion of sustainability related items. Waypoint is committed to transparency by publicly reporting its gender pay ratio and gender pay gap on an annual basis.

### **Professional development**

We are committed to providing our employees with opportunities for learning and development, including in relation to Environmental, Social and Governance issues, through:

- On-the-job work/doing the job at hand;
- Formal in-house or external training to improve a skill or increase expertise;
- Subsidising in whole or part relevant examination qualifications and membership of professional bodies; and
- Coaching through direct feedback from a supervisor, peer or mentor.

### **ESG communications and training**



We communicate our Environmental, Social and Governance (ESG) commitment to all employees, so that all employees are aware of the commitments made and their role in helping achieve our ESG goals. Internal and external ESG training is provided or made available to all appropriate staff.

### **Diversity, equity and inclusion**

We aim to create a work environment that reflects the goals and values of clients and investors we serve, provides everyone with the opportunity to succeed, values the differences of each individual and recognises their contributions to the success of our business.

The ways in which we seek to achieve this objective are set out in detail in our Diversity, Equity and Inclusion policy.

### **Procurement**

We have a responsibility to procure goods and services at a reasonable cost and, where such costs are recovered from our tenants through a service charge, to provide value for money. Within these parameters we work, where appropriate, with suppliers local to areas in which our properties are situated and, when procuring services, will ensure that local companies are given an opportunity to participate in tenders and to quote on an equal footing.

When goods and services are procured on our behalf by our external property managers and in agreeing to forward fund new developments, we will use our influence to ensure that local suppliers and contractors are given an equal opportunity to tender for work, whenever it is appropriate.

### **Governance**

Our corporate operations are overseen by our board of directors, and our investment activities are overseen by an Investment Committee chaired by a Board member. These committees work together to ensure proper execution of our investment strategies, consistent application of our policies, compliance with our procedures and compliance with local and regional regulatory requirements.

The board is responsible for setting our strategic direction, for establishing appropriate investment programmes and for designing and implementing the policies and procedures that govern our operations, including our ESG practices.

Our approach to good governance is set out in detail in our various policies, which are set out in the Appendix and, for the purposes of this policy, is summarised below:

### **Compliance**

We are committed to conducting business with the highest integrity and in compliance with the letter and spirit of the law. All employees must adhere to our management policies and procedures.



The Compliance Officer is a member of our board and is primarily responsible for ensuring the implementation, monitoring, review and enforcement of our policy and procedures.

The Compliance Officer implements and oversees legal and regulatory compliance and risk management. Responsibilities include, among other things, ensuring compliance in relation to regulatory filings, reviewing, updating and maintaining policies, advising on new laws and reviewing conflicts of interest.

Every employee undergoes training so that they are informed of their compliance obligations and how to identify compliance issues.

## **Risk Management**

Our governance model is designed to manage both, investment and operational risks.

- **Investment Risk**

Investment risk is overseen by the appropriate Investment Committee which monitors all capital transactions undertaken by the relevant fund. These committees ensure that proper emphasis is placed on preservation of capital, identification and management of investment risk and appropriate pricing of risk at the portfolio and property level.

The Waypoint Board is responsible for monitoring portfolio risk across the business and reviewing each of the investment portfolios on a quarterly basis.

- **Operational Risk**

Our Compliance Officer reports to the board, and is tasked with identifying, capturing, assessing, managing and monitoring the operational risks including litigation, insurance and regulatory compliance, tax and IT disaster recovery procedures.

## **Reporting**

We recognise the importance of setting targets for the management of ESG, for mitigating sustainability-related risks and for the exploitation of opportunities to add value. We set long term targets for key initiatives and monitor progress year on year.

Our fund managers make a report on each fund's progress to the relevant investment or Advisory Committees, together with our Board, on a quarterly basis, and a section on sustainability is included in our formal annual reports to investors in our funds.

We recognise the importance of benchmarking the performance of our assets against other investment properties and the performance of funds under our management with other funds. To this end, we submit all our directly controlled funds to the Global Real Estate Sustainability Benchmark (GRESB).

We continuously monitor and assess the applicability of sustainability-related frameworks and standards at global, regional, and domestic levels, including:

- ISSB and TCFD Standards



- SBTi framework
- EU Taxonomy
- PCAF
- UK FCA SDR & EU SFRD

## **Adoption of Sustainable Practices by Third Parties**

As a business, we recognise that we do not always have direct control over sustainable best practice, but we do acknowledge that we have a duty to influence positive behaviour amongst our stakeholders including client's, occupiers and third-party suppliers. Where we identify that a third-party's actions or requests are in direct contravention to our own policy and potentially damaging, then the matter is to be reported to both the Sustainability Committee and Main Board for direction on an appropriate course of action.

## **Annual Review Requirements**

We recognise that sustainability practice is constantly evolving and to reflect this a summary of our annual commitments is set out below:

- Review of ESG Policy
- Individual Fund level GRESB submissions
- Corporate Annual Sustainability Strategy & Report (published on our website).
- UN PRI Signatory status and reporting framework
- Net Zero pathways and progress against targets at both a fund and corporate level
- Staff training programme

Nick Gregory  
Joint Managing Director  
Waypoint Asset Management Limited

*Annual review date: 02/12/2025*

## **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 gender-based 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 the Disciplinary Procedure.

Waypoint recognises its obligations to take pre-emptive action in relation to sexual harassment in the workplace under the Equality Act 2010, which extends to cover:

- work-related activities outside Waypoint's premises;
- the conduct of third parties engaged by Waypoint.



Waypoint will carry out risk assessments and put reasonable preventative measures in place. All Waypoint staff are encouraged to bring forward suggestions (if felt necessary, in confidence) to assist in preventing such situations from arising.

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 staff are required to co-operate with efforts to ensure that the policy is implemented in full. This includes the supervision of Waypoint's managing 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



should pursue the matter through the Grievance Procedure including, if necessary in the circumstances, making use of the Whistleblowing Procedure.

Waypoint tracks and reports on the representation of gender, ethnicity and age within its workforce as part of its ongoing commitment to the development of policy in this area.

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.

**Nick Gregory**  
**Joint Managing Director**  
**Waypoint Asset Management Limited**

*Annual review date: 21/08/2025*

## **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. In applying this approach, Waypoint takes account of both its environmental social and governance (“ESG”) commitments and the findings of the employee satisfaction and wellbeing surveys it carries out on a periodic basis.

##### **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.

In determining the appropriate balance between office-based and remote working, Waypoint takes account of the need for development of team culture, fostering a mutually supportive environment and the personal development needs of individuals.

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-life 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.

The approach set out in this policy is designed to reflect, in particular, the following Waypoint policies, some of which are contained in the Staff Handbook:

- Anti-Bribery
- Anti-Money Laundering
- Environmental, Social and Governance
- Complaints Handling
- Conflicts of Interest
- Criminal Finances
- Deal Allocation
- Diversity, Equity & Inclusion
- Health, Safety & Welfare
- Maternity, Paternity & Family
- Treating Customers Fairly
- Whistleblowing

**Nick Gregory**  
Joint Managing Director  
Waypoint Asset Management Limited

*Annual review date: 21/08/2025*

## WAYPOINT MODERN SLAVERY AND CHILD LABOUR POLICY

### Introduction and Policy Statement

The directors of Waypoint Asset Management Limited, Waypoint Capital Limited and their subsidiary and associate businesses (“**Waypoint**”) have adopted the policy contained in this document in recognition of Waypoint’s commitment to fulfilling the requirements and spirit of the Modern Slavery Act 2015 (the “**2015 Act**”). This document comprises Waypoint’s human trafficking and slavery statement for the purposes of the 2015 Act, together with Waypoint’s policy towards the use of child labour, including alignment with the standards promulgated by the International Labour Organisation (“**ILO**”).

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 its Anti-Financial Crime policies and procedures.

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 ILO standards regarding the employment of children and young people in relation to work that:

- is mentally, physically, socially or morally harmful to children; and/or
- interferes with their schooling by depriving them of the opportunity to attend school, obliging them to leave school prematurely or requiring them to attempt to combine school attendance with excessively long and heavy work.

Waypoint will not trade or partner with any business or organisation that knowingly has any connection with such practices, however indirectly.

For employment in UK businesses, this includes:

(a) not employing anyone under the age of completion of compulsory schooling, and in any case not before the age of 15; and

(b) employees under the age of 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 managers, 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 and child labour is also very low. Again, we will disassociate ourselves from any supplier found to be knowingly connected to modern slavery practices.

### **Action**

We expect our suppliers to join us in taking a zero-tolerance attitude in this area. To this end, 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 and ILO standards on child slavery. We also reviewed our other governance policies to assure ourselves that they support this policy statement.

We also 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.

### **Ongoing Approach**

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.



## **Review**

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.

A handwritten signature in black ink, appearing to read "Nick Gregory".

**Nick Gregory**  
**Joint Managing Director**  
**Waypoint Asset Management Limited**

*Annual review date: 01/12/2025*

## 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 staff members 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.



Nick Gregory  
Joint Managing Director  
Waypoint Asset Management Limited

*Annual review date: 31/03/2025*

## WAYPOINT RESPONSIBLE INVESTMENT AND STEWARDSHIP POLICY

### 1. Introduction

The directors of Waypoint Asset Management Limited, Waypoint Capital Limited and their subsidiary and associate businesses (“Waypoint”) have adopted the following policy in relation to conducting Waypoint’s investment activities in a responsible manner.

Waypoint is a real estate asset manager and investment adviser that creates and executes innovative and bespoke investment strategies for clients. We advise on over £3.5bn 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.

The UK Stewardship Code 2020 (the “Code”), focussed on entities listed on public markets together with their sponsors and fund managers, is not directly applicable to Waypoint. However, we consider that our policies and procedures reflect and are supportive of the principles of the Code that are applicable to us 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.
- Reduce Waypoint’s corporate greenhouse gas emissions by 50% by 2030.
- Reduce Waypoint’s corporate greenhouse gas emissions by 75% by 2040.
- Offset where it is no longer possible to further reduce Waypoint’s outstanding greenhouse gas emissions.
- Achieve 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.
- Support our clients in achieving their individual carbon reduction goals.

### **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 issues - 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.

Nick Gregory  
Joint Managing Director  
Waypoint Asset Management Limited

*Annual review date: 01/12/2025*

## WAYPOINT ETHICAL CONDUCT POLICY

Waypoint is committed to acting ethically in conducting its business. This over-arching concept is achieved through every staff member acting in an ethical way and accepting personal responsibility for their actions in all of their dealings. The interests of Waypoint's clients are paramount and should be placed above those of Waypoint and the individual employee.

In relation to this, you must 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  
Data Protection  
Complaints Handling

Deal Allocation  
Anti-Financial Crime  
Responsible Investment  
Responsible Procurement

Copies of these policies have been provided to you and may be found in the Waypoint policy suite at WAM - U\01 STAFF RESOURCE HUB\01 SH and Policy Suite.

Staff working on activities for Waypoint Investment Management Limited ("WIML") must also adhere to relevant policies and procedures contained in the WIML Compliance Manual, with which they have been provided and which is also available on the SH and Policy Suite.

If you are in doubt as to the appropriate course of action in any instance, please direct any questions to the Compliance Officer.



**Nick Gregory**  
**Joint Managing Director**  
**Waypoint Asset Management Limited**

*Annual review date: 15/01/2026*