Version Updated
January 2026

Corporate Compliance Manual

Contents

Anti Bribery and Corruption

1. Policy statement

1.1 Alpha conducts all its business in an honest and ethical manner. We take a zero-tolerance approach to bribery and corruption and are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter bribery and corruption.

1.2 We take our legal responsibilities very seriously. We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate. In particular, we are bound by UK laws, including the Bribery Act 2010, in respect of our conduct both in the UK and abroad.

2. About this policy

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and of those working for and on our behalf, in observing and upholding our position on bribery and corruption; and

(b) provide information and guidance to those working for and on our behalf on how to recognise and deal with bribery and corruption issues.

2.2 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

3. Who does this policy apply to?

This policy applies to all persons working for any Alpha group company or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located.

4. Who is responsible for the policy?

4.1 The board of directors (the Board) has overall responsibility for the effective operation of this policy but has delegated responsibility for overseeing its implementation to the Global Head of Legal and Corporate Affairs. Suggestions for change should be reported to the Global Head of Legal and Corporate Affairs.

4.2 This policy is reviewed regularly by the Global Head of Legal and Corporate Affairs, the Global Head of Risk and other senior executives.

5. Definitions

5.1 **Bribery** is offering, promising, giving or accepting any financial or other advantage, to induce the recipient or any other person to act improperly in the performance of their functions, or to reward them for acting improperly, or where the recipient would act improperly by accepting the advantage.

(a) An **advantage** includes money, gifts, loans, fees, hospitality, services, discounts, the award of a contract or anything else of value.

(b) A person acts **improperly** where they act illegally, unethically, or contrary to an expectation of good faith or impartiality, or where they abuse a position of trust. It is a criminal offence to offer, promise, give, request, or accept a bribe. Individuals found guilty can be punished by up to ten years' imprisonment and/or a fine and employers that fail to prevent bribery can face an unlimited fine, exclusion from tendering for public contracts, and damage to its reputation.

5.2 **Corruption** is the abuse of entrusted power or position for private gain.

Examples:

Offering a bribe: You offer a potential client tickets to a major sporting event, but only if they agree to do business with us.

You would be committing an offence as you are making the offer to gain a commercial and contractual advantage. Alpha may also be found to have committed an offence because the offer has been made to obtain business for Alpha. It may also be an offence for the potential client to accept your offer.

Receiving a bribe: A supplier gives your relative a job but makes it clear that in return they expect you to use your influence in Alpha to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

Bribing a foreign official: You arrange for the business to pay an additional "facilitation“ payment to a foreign official to speed up an administrative process, such as a required regulatory clearance.

The offence of bribing a foreign public official is committed as soon as the offer is made. This is because it is made to gain a business advantage for Alpha. Alpha may also be found to have committed an offence.

Anti Bribery and Corruption

5.3 **Facilitation payments**, also known as "back-handers" or "grease payments", are typically small, unofficial payments made to secure or expedite a routine or necessary action (for example by a government official). They are not common in the UK but are common in some other jurisdictions.

5.4 **Kickbacks** are typically payments made in return for a business favour or advantage.

5.5 **Third party** means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

6. **Identifying risks of bribery and corruption**

6.1 We have identified that the following may be risk areas for our business:

6.1.1 relationships with existing and potential clients;

6.1.2 relationships with vendors and suppliers of good and services;

6.1.3 partnership arrangements with third parties; and

6.1.4 business activities in certain jurisdictions.

These risks are monitored as part of the broader periodic corruption risk assessment which is performed by members of the Risk, Finance and Legal teams, and anything outside of the course of usual business is reported to the Chief Financial Officer for further investigation.

7. **What you must not do**

It is not acceptable for you (or someone on your behalf) to:

(a) give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;

(b) give or accept a gift or hospitality during any commercial negotiations or tender process, if this could be perceived as intended or likely to influence the outcome;

(c) accept a payment, gift or hospitality from a third party that you know or suspect is offered with the expectation that it will provide a business advantage for them or anyone else in return;

(d) offer or accept a gift to or from government officials or representatives, or politicians or political parties; or

(f) threaten or retaliate against another individual who has refused to commit a bribery offence or who has raised concerns under this policy; or

(e) engage in any other activity that might lead to a breach of this policy.

8. **Facilitation payments and kickbacks**

8.1 We do not make, and will not accept, facilitation payments or "kickbacks" of any kind. See clause 5 for definitions of these terms.

8.2 You must avoid any activity that might lead to a facilitation payment or kickback being made or accepted by us or on our behalf, or that might suggest that such a payment will be made or accepted. If you are asked to make a payment on our behalf, you should always be mindful of what the payment is for and whether the amount requested is proportionate to the goods or services provided. You should always ask for a receipt which details the reason for the payment. If you have any suspicions, concerns or queries regarding a payment, you should raise these with the Global Head of Legal and Corporate Affairs.

9. Provision of Gifts and Hospitality to Clients and third parties

9.1 This policy allows reasonable and appropriate hospitality or entertainment given to client and prospective clients, for the purposes of:

(a) establishing or maintaining good business relationships;

(b) marketing or presenting our products and/or services effectively.

9.2 The making of gifts is allowed only if the following requirements are met:

(a) it is not made with the intention of influencing a third party to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits;

(b) it is given in Alpha's name, not in your name;

(c) it does not include cash or a cash equivalent (such as gift certificates or vouchers);

(d) it is appropriate in the circumstances, taking account of the reason for the gift, its timing and value. For example, in the UK it is customary for small gifts to be given at Christmas;

(e) it is given openly, not secretly; and

(f) it complies with any applicable local law.

Anti Bribery and Corruption

9.3 Entertainment or hospitality provided that exceeds internally defined thresholds requires the prior written approval of the Global Head of Legal and Corporate Affairs. If this limit is inadvertently exceeded, then retrospective approval must be sought from the Global Head of Legal and Corporate Affairs. In addition, entertainment may also require the approval of an Executive Director. Pleas refer to internal thresholds for information.

9.4 Promotional gifts of low value such as branded stationery to or from existing customers, suppliers and business partners will usually be acceptable.

9.5 We appreciate that practice varies between countries and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift, hospitality or payment is reasonable and justifiable. The intention behind it should always be considered.

10. Receipt of Gifts and Hospitality from Third Parties

10.1 It is the responsibility of all staff to ensure that no gifts or entertainment are received, or requested from, third parties (for example, suppliers or contractors) that may be considered to be bribes.

10.2 All gifts or entertainment received with a monetary value over internally defined thresholds must be reported to the Global Head of Legal and Corporate Affairs by sending an email to the following address antibribery@alphafmc.com. If the Global Head of Legal and Corporate Affairs considers that the gifts or entertainment could be interpreted as bribes, then the gifts will be required to be returned (or donated to charity)/or the entertainment declined. There is weekly monitoring of gifts and entertainment across the firm to ensure that limits are adhered to, and that anything outside of policy has received the proper pre-approval.

11. Donations

11.1 We do not make contributions to political parties.

11.2 Generally, we do not make charitable donations and, when we do, we must ensure that they are legal and ethical under local laws and practices. If you wish Alpha to consider making a charitable donation, please provide details to either the Global Head of Legal and Corporate Affairs, the Global Head of Risk or the Managing Director. You should not agree to make any donation without the specific written approval of one of these individuals.

12. Record-keeping

12.1 We must keep financial records and have appropriate internal controls in place which will evidence the business reason for making payments to third parties.

12.2 The Finance team and the Global Head of Legal and Corporate Affairs will monitor expenses and identify and review instances where the spending limits set out above have been exceeded.

12.3 All accounts, invoices, and other records relating to dealings with third parties including suppliers and customers should be prepared with strict accuracy and completeness. Accounts must not be kept "off-book" to facilitate or conceal improper payments.

13. Your responsibilities

13.1 You must ensure that you read, understand and comply with this policy. If you have any questions in respect of the policy, please email: antibribery@alphafmc.com.

13.2 You must complete the Anti-Bribery and Corruption training and pass the related test on an annual basis.

13.3 The prevention, detection and reporting of bribery and other forms of corruption are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

13.4 You must notify the Global Head of Legal and Corporate Affairs as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. Examples of "red flags" that may indicate bribery or corruption are set out in clause 188.

Anti Bribery and Corruption

14. How to raise a concern

14.1 You are encouraged to raise concerns about any issue or suspicion of bribery or corruption at the earliest possible stage.

14.2 If you are offered a bribe, or are asked to make one, or if you believe or suspect that any bribery, corruption or other breach of this policy has occurred or may occur, you must notify the Global Head of Legal and Corporate Affairs or report it in accordance with our Whistleblowing Policy as soon as possible.

14.3 If you are unsure about whether a particular act constitutes bribery or corruption, raise it with the Global Head of Legal and Corporate Affairs or email antibribery@alphafmc.com.

15. Protection

15.1 Individuals who refuse to accept or offer a bribe, or who raise concerns or report another's wrongdoing, are sometimes worried about possible repercussions. We aim to encourage openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken.

15.2 We are committed to ensuring no one suffers any detrimental treatment as a result of refusing to take part in bribery or corruption, or because of reporting in good faith their suspicion that an actual or potential bribery or other corruption offence has taken place or may take place in the future. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment connected with raising a concern. If you believe that you have suffered any such treatment, you should inform a member of the HR team immediately. If the matter is not remedied, and you are an employee, you should raise it formally using our Grievance Procedure, which is available in the Employee Handbook.

16. Training and communication

16.1 Training on this policy forms part of the induction process for all individuals who work for us, and regular training and testing will be provided at least annually.

16.2 Our zero-tolerance approach to bribery and corruption must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate thereafter.

17. Breaches of this policy

17.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

17.2 We may terminate our relationship with other individuals and organisations working on our behalf if they breach this policy.

18. Potential risk scenarios: "red flags"

The following is a list of possible red flags that may arise during the course of you working for us and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only. If you encounter any of these red flags while working for us, you must report them promptly to the Global Head of Legal and Corporate Affairs or using the procedure set out in the Whistleblowing Policy:

(a) a third party insists on receiving a commission or fee payment before committing to sign up to a contract with us, or carrying out a government function or process for us;

(b) a third party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made;

c) a third party requests that payment is made to a country or geographic location different from where the third party resides or conducts business;

(d) a third party requests an unexpected additional fee or commission to "facilitate" a service;

(e) a third party demands lavish entertainment or gifts before commencing or continuing contractual negotiations or provision of services;

(f) a third party requests that a payment is made to "overlook" potential legal violations;

(g) a third party requests that you provide employment or some other advantage to a friend or relative;

(h) you receive an invoice from a third party that appears to be non-standard or customised;

(i) a third party insists on the use of side letters or refuses to put terms agreed in writing;

(j) a third party requests or requires the use of an agent, intermediary, consultant, distributor or supplier that is not typically used by or known to us; or

(k) you are offered an unusually generous gift or offered lavish hospitality by a third party.

Issued: November 2022

Amended: April 2025

Anti-Money Laundering Principles

The Alpha FMC group has principles which it considers to be appropriate and proportionate to comply with anti-money laundering regulations ("AML Regulations") in the jurisdictions in which it operates.1.2 We take our legal responsibilities very seriously. We will uphold all laws relevant to countering bribery and corruption in all the jurisdictions in which we operate. In particular, we are bound by UK laws, including the Bribery Act 2010, in respect of our conduct both in the UK and abroad.

Money laundering is the illegal process of making money, generated by criminal activity, appear to have come from a legitimate source. It typically involves 3 stages:

- Placement (i.e. moving the funds from direct association with the crime)
- Layering (i.e. disguising the trail to foil pursuit)
- Integration (i.e. making the money available to the criminal from what seem to be legitimate sources)

This policy applies to all persons working for any Alpha group company or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located.

Alpha employees must complete the AML training and pass the associated test on an annual basis.

Common Money Laundering Risks

1. Unusual transactions: Unexplained payments from a third party or an account in an unconnected country.

2. Ultimate beneficial ownership is unclear: Ultimate beneficial owners are the people who ultimately own or manage a company. Complex ownership structures, where ownership is unclear, could be an attempt to disguise criminal activities.

3. Jurisdiction risk: Some countries have high levels of corruption, unstable governments, or are known as money laundering havens.

4. Adverse media: Negative news media may highlight criminal activity.

To ensure compliance with applicable AML Regulations the following principles are adhered to:

Customer due diligence: Steps are taken to verify the identity of clients and understand their activities to assess money laundering risks:

- Sanctions checks and adverse media screening
- Credit checks, conducted by a third-party provider
- Client base is monitored using business line client onboarding assessments, operational service delivery reviews and finance routine activities.

A periodic corruption risk assessment is also performed by members of the Risk, Finance and Legal teams, and anything outside of the course of usual business is reported to the Chief Financial Officer for further investigation.

Transaction monitoring: Alpha does not hold client money and so this area is low risk. However, procedures are in place:

- Checking that sender name matches expected payor
- Querying any unexpected payments/payments that do not match an invoice which has been issued
- Validating invoices with the person or business area receiving the service
- Alpha does not accept money outside normal client invoicing
- If Alpha makes a charitable donation the destination and use of the donation will be verified

Record keeping: Records of transactions and customer information are retained for at least 6 years.

Staff must comply with any client specific money laundering policies which they are required to under the terms of Alpha's engagement with that client.

Any concerns regarding potential money laundering should be immediately raised with one of the following:

- Chief Financial Officer
- Group Head of Legal and Corporate Affairs
- Group Head of Risk and Responsible Business

Issued: January 2025

Anti-Facilitation of Tax Avoidance and Financial Crime Policy

1 POLICY STATEMENT

1.1 Tax evasion and broader economic crimes recognised by the Economic Crime and Corporate Transparency Act 2023 (ECCTA) are major issues in world trade and are very damaging to the societies in which it occurs. Tax evasion and ECCTA-included crimes (detailed in Section 5) affect Alpha ("we") as an organisation if they are criminally facilitated anywhere in our business.

1.2 We are committed to acting professionally, fairly and with integrity in all our business dealings and relationships wherever we operate and implementing and enforcing effective systems to counter tax evasion facilitation and other financial crimes recognised by the ECCTA.

1.3 This policy is a crucial element of that effort. Alpha does not tolerate tax evasion, the criminal facilitation of tax evasion, or any other economic crime within its business. We expect all our employees, whether providing client services or providing administrative support, to conduct themselves in accordance with this policy.

1.4 Alpha will uphold all laws relevant to countering tax evasion in all the jurisdictions in which we operate, including the UK Criminal Finances Act 2017 and the Economic Crime and Corporate Transparency Act 2023.

2 ABOUT THIS POLICY

2.1 The purpose of this policy is to: (a) set out our responsibilities, and of those working for Alpha, in observing and upholding our position on preventing the criminal facilitation of tax evasion and other financial crimes recognised by the ECCTA ("economic crime", "financial crime" or analogues in this document); and

(b) provide information and guidance to those working for us on how to recognize and avoid such criminal activities.

2.2 This policy applies to all people working for any Alpha Group or on our behalf in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, contractors, external consultants, third-party representatives and business partners or any other person associated with us, wherever located.

2.3 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

3 MONITORING AND REVIEW

3.1 Alpha Financial Markets Consulting's Board of Directors has delegated to the Global Coordination Committee the overall responsibility for ensuring this policy complies with our legal and ethical obligations, and that all those under our control comply with it.

3.2 The Chief Financial Officer has primary and day-to-day responsibility for implementing this policy, monitoring its use and effectiveness, dealing with any queries about it, and auditing internal control systems and procedures to ensure they are effective in preventing the facilitation of tax evasion and other economic crimes.

4 WHAT IS TAX EVASION AND ITS FACILITATION?

4.1 Tax evasion means the illegal non-payment or under-payment of taxes and is a criminal offence. The offence requires an element of fraud, which means there must be deliberate action, or omission with dishonest intent. Circumstances in which tax evasion may occur in relation to our business include structuring a transaction on behalf of a client in such a way as to evade tax, or if a supplier asks us to pay them cash in hand or via some complex payment mechanism that allows them to evade tax.

4.2 Under the Criminal Finances Act 2017, a separate criminal offence is automatically committed by a corporate entity where the tax evasion is facilitated by a person acting in the capacity of an "associated person" to that body. The offence has three ingredients, all of which must exist for criminal liability to arise:

(a) criminal tax evasion by a taxpayer e.g. by a client or supplier of Alpha;

(b) criminal facilitation of that tax evasion by Alpha's employee, agent, or any other person performing services on our behalf. This means they must deliberately and dishonestly take action to facilitate the tax evasion; and

(c) failure by Alpha to prevent our employee, agent etc. from committing the criminal facilitation.

4.3 This offence can be committed regardless of whether the tax evaded is owed in the UK or in a foreign country.

4.4 There is only one relevant defence to the corporate offence of failure to prevent the criminal facilitation of tax evasion - the defence is that when the tax evasion facilitation offence was committed, Alpha had reasonable prevention policies in place. This policy is central to those prevention procedures.

4.5 Tax "evasion" is not the same as tax "avoidance" or tax planning. Tax evasion involves deliberate and dishonest conduct. Tax avoidance is not illegal and involves taking steps, within the law, to minimise tax payable (or maximising tax reliefs).

5 WHAT IS THE ECONOMIC CRIME AND CORPORATE TRANSPARENCY ACT 2023?

5.1 The Economic Crime and Corporate Transparency Act 2023 (ECCTA) strengthens corporate criminal liability by expanding the responsibilities of companies to prevent economic crimes, including

Anti-Facilitation of Tax Avoidance and Financial Crime Policy

fraud, money laundering, and false accounting.

5.2 A key provision of the ECCTA is the corporate “failure to prevent fraud” offence, which holds organisations criminally liable if an employee, agent, or associated person commits fraud for the benefit of the organisation and the organisation did not have reasonable prevention measures in place.

5.3 Fraud under the ECCTA can include:

(a) false accounting;

(b) fraudulent trading;

(c) misrepresentation with the intention to deceive a tax authority or other body; and

(d) other offences as defined under the Fraud Act 2006 and related legislation.

5.4 As with tax evasion facilitation, Alpha has a zero-tolerance approach to fraud and financial crime. We are committed to implementing reasonable prevention procedures to comply with the ECCTA and to mitigate risks related to economic crime.

5 RISK ASSESSMENT

5.1 Alpha has conducted an organisation-wide assessment of the areas where we feel there is most risk of involvement in the facilitation of tax evasion and economic crime, and that assessment has been documented.

5.2 Whilst overall the assessment indicates that the risk to Alpha is low, mitigation and monitoring steps have been implemented.

5.3 Risk is continually monitored, particularly in respect of external developments and changes in the organisation’s activities.

6 WHAT YOU MUST NOT DO

6.1 It is not acceptable for you (or someone on your behalf) to:

(a) engage in any form of facilitating tax evasion or foreign tax evasion;

(b) aid, abet, counsel or procure the commission of a tax evasion offence or foreign tax evasion offence by another person;

(c) fail to promptly report any request or demand from any third party to facilitate the fraudulent evasion of tax (whether UK tax or tax in a foreign country), or any suspected fraudulent evasion of tax (whether UK tax or tax in a foreign country) by another person, in accordance with this policy;

(d) engage in any other activity that might lead to a breach of this policy; or

(e) threaten or retaliate against another individual who has refused to commit a tax evasion offence or a foreign tax evasion offence or who has raised concerns under this policy.

7 YOUR RESPONSIBILITIES

7.1 You must ensure that you read, understand and comply with this policy.

7.2 The prevention, detection and reporting of tax evasion and foreign tax evasion are the responsibility of all those working for us or under our control. You are required to avoid any activity that might lead to, or suggest, a breach of this policy.

7.3 You must notify the Chief Financial Officer or Global Head of Legal and Corporate Affairs as soon as possible if you believe or suspect that a conflict with this policy has occurred or may occur in the future. For example, if an employee or supplier asks to be paid into an offshore bank account, without good reason, or a supplier asks to be paid in cash, indicating that this will mean the payment is not subject to VAT. Further "red flags" that may indicate potential tax evasion or foreign tax evasion are set out in paragraph 11 of this policy.

8 WHAT TO DO IF YOU THINK SOMETHING IS WRONG

8.1 Each of us has a responsibility to speak out if we discover anything corrupt or otherwise improper occurring in relation to our business. You are encouraged to raise concerns about any issue or suspicion of financial crime at the earliest possible stage.

8.2 If you discover or suspect that a financial crime has been facilitated or is being facilitated, whether by:

(a) another staff member;

(b) a third party who represents us;

(c) one of our suppliers; or

(d) anyone else, perhaps even a client, you must notify the Global Head of Legal and Corporate Affairs or the Chief Financial Officer or report it in accordance with our Whistleblowing Policy, which can be found in the employee handbook, as soon as possible.

8.3 If you are unsure about whether a particular act constitutes a financial crime, raise it with your team Director or Mentor or the Chief Financial Officer as soon as possible. You should note that the corporate offence is only committed when you deliberately and dishonestly take action to facilitate the financial crime. However, a deliberate failure to report suspected financial crime, or "turning a blind eye" to suspicious activity could amount to criminal facilitation of financial crime.

8.4 Individuals who raise concerns or report another's wrongdoing may be worried about facing possible repercussions. Alpha encourages openness and will support anyone who raises genuine concerns in good faith under this policy, even if they turn out to be mistaken. All matters raised will be dealt with in strict confidence and you will not suffer any adverse consequence for refusing to engage in the facilitation of financial crime or for reporting instances in which you suspect that this policy has been breached, even if this may result in Alpha losing business.

9 TRAINING AND COMMUNICATION

9.1 Training on this policy will form part of the induction process for all individuals who work for us, and further training will be provided as necessary. Such training may form part of wider financial crime detection and prevention training.

9.2 If you have questions at any time in relation to the offence or this policy, or you feel that you would benefit from further training in relation to them, please contact the Chief Financial Officer, Global Head of Risk or the Global Head of Legal and Corporate Affairs.

9.3 Our zero-tolerance approach to financial crime must be communicated to all suppliers, contractors and business partners at the outset of our business relationship with them and as appropriate after that.

10 CONSEQUENCES OF FAILING TO COMPLY

10.1 We take compliance with this policy very seriously, as failure to comply puts both you and Alpha at risk.

10.2 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct. Any non-employee who breaches this policy is liable to have their contract terminated with immediate effect.

11 POTENTIAL RISK SCENARIOS: "RED FLAGS"

11.1 The following is a list of possible red flags that may arise while you for us and which may raise concerns related to tax evasion or financial crime under the ECCTA. The list is not intended to be exhaustive and is for illustrative purposes only.

11.2 If you encounter any of these red flags while working for us, you must report them promptly to your manager or the Chief Financial Officer or report using the procedure set out in our Whistleblowing Policy:

(a) False Statements and Hidden Income

i. A third party has made or intends to make a false statement relating to tax or has failed to disclose income/gains to HMRC.

ii. A third party delivers or intends to deliver a false document relating to tax or sets up a structure to hide income, gains, or assets from a tax authority.

(b) Invoicing Irregularities

i. A client requests to amend their Statement of Work to change the entity we are invoicing to one not involved in the project in a jurisdiction where VAT would not be chargeable.

ii. A third party requests that their invoice is addressed to a different entity where we did not provide services directly.

iii. A third party asks us to change the description of services rendered in a way that obscures the nature of the services provided.

iv. Receiving an invoice that appears to be non-standard or customized.

v. We have been invoiced for a commission or fee payment that appears too large or too small for the service provided.

vi. A third party insists on the use of side letters or refuses to put terms in writing or requests backdated documents.

(c) Cash Payments and Documentation Issues

i. A third-party requests payment in cash and/or refuses to sign a formal commission or fee agreement or provide an invoice/receipt.

ii. A third party working for us as an employee asks to be treated as a self-employed contractor without changes to their working conditions.

iii. A supplier or subcontractor is paid gross when they should have been paid net under applicable schemes.

(d) Unusual Payment Requests

i. A third party requests that payment is made to a different country or geographic location.

ii. A third party requests or requires the use of an agent, intermediary, or consultant not typically known to us.

Anti-Facilitation of Tax Avoidance and Financial Crime Policy

iii. Receiving payments from multiple accounts with no clear business rationale.

(e) Complex Structures and Lack of Transparency

i. Requests to set up shell companies, nominee arrangements, or complex corporate structures without clear commercial justification.

ii. Sudden or unexplained changes in a client's ownership structure involving offshore entities.

iii. A third party refuses to disclose sources of funds or insists on payments from unrelated accounts.

iv. A third party refuses to provide details about ultimate beneficial ownership when required.

(f) Pressure and Due Diligence Concerns

i. Undue pressure from clients or third parties to expedite processes that normally require enhanced due diligence.

ii. A client requests that we perform due diligence but asks to omit verification steps or ignore discrepancies in ownership records.

(g) Suspicious Documentation

i. A supplier or subcontractor provides inconsistent, forged, or suspicious documentation related to payments or ownership.

Alpha Global Coordination Committee

Issued: December 2019

Updated: July 2025

Sanctions Policy

1. **Introduction**

1.1 Alpha is committed to carrying on business in accordance with the highest ethical standards. This includes complying with all applicable trade sanctions regulations (“Sanctions“) in the countries in which we operate.

1.2 Any employee who violates the rules in this Policy, or who encourages or assists anyone to do so, may be subject to appropriate disciplinary action, up to and including dismissal. Employees may also be subject to personal civil or criminal fines imposed by applicable State laws.

1.3 If you have any questions about this Policy, you should contact the Global Head of Legal and Corporate Affairs or the Global Head of Risk.

2. **Policy Statement**

2.1 It is Alpha’s policy to comply with all Sanctions in our business operations worldwide. Accordingly, Alpha will comply with all economic and trade sanctions which apply to our business activities.

2.2 No person will receive detrimental treatment from Alpha senior management for any loss of business which results from complying with this Policy.

3. **Who is subject to this Policy?**

3.1 This Policy applies to Alpha Group’s operations globally, and to all directors, employees, contractors, and other third parties acting on behalf of the foregoing.

4. **What is the risk?**

4.1 Violations of Sanctions may lead to severe civil and/or criminal penalties against companies and individuals, including significant monetary fines, imprisonment, extradition, revocation of licenses and disqualification of directors.

4.2 Sanctions violations can also damage reputation and harm commercial relationships.

5. **What are “Sanctions”?**

5.1 Sanctions are the regulatory restrictions applicable to dealings with certain countries/territories (**“Restricted Territories”**), governments, groups, entities, individuals (**“Restricted Parties”**), or controlled goods or services (**“Restricted Items”**). These restrictions, and their scope, change over time. You should therefore consult with the Legal Department to understand the business implications.

5.2 The following are some examples of groups and items that have been the target of economic trade sanctions: narcotics traffickers, Weapons of Mass Destruction, human rights abusers and terrorists, among others.

5.3 This list is **not** meant to be exhaustive and may change over time in line with global regulatory and legal requirements.

6. **How do we ensure compliance with sanctions?**

6.1 Alpha employees and contractors must comply with this Policy in respect of all business-related activities. The potential restrictions imposed by Sanctions may be related to:

- **Where** we do business: ensuring compliance with sanctions on Restricted Territories;

- **Who** we do business with: ensuring compliance with sanctions on Restricted Entities;

- **How** we do business: ensuring we do not circumvent, evade, or facilitate the contravention of sanctions rules; and

- **Red flags**: ensuring we report any suspicions which may raise sanctions concerns.

6.2 If you are in any doubt or have any questions or concerns, please contact the Legal Department before proceeding further.

7. **Red Flags**

7.1 There are a number of issues, which should cause us to conduct further investigation into whether a particular transaction or relationship may present a potential economic trade sanctions regulation issue.

7.2 Alpha employees and contractors must be alert to any red flags or suspicions that may indicate the direct or indirect involvement of a Restricted Territory, Restricted Entity, Restricted Item, service, end-use or any other sanctions compliance concern.

7.3 Some examples of red flags to be reported include:

- The customer is reluctant to offer information or clear answers on routine commercial issues (including intended geography of services, beneficial ownership, or locations of operation);

- Unusual invoicing requests;

- Unusually favourable payment terms or large cash payments;

- Any suspicion or evidence to suggest the possible involvement of a Restricted Territory or Restricted Party;

Sanctions Policy

The above is not intended to be an exhaustive list. Any suspicion of the direct or indirect involvement of a Restricted Territory, Restricted Party, Restricted Item, service, end-use or any other sanctions compliance concern should alert you to raise the matter with the Legal team to investigate the activity in accordance with this Policy.

8. Compliance controls

8.1 The responsibility to provide Alpha employees with the necessary information to comply with this Policy falls with Legal, Finance and Risk, as below:

Legal

- Monitors economic trade sanctions regulations.

- Provides legal advice and guidance on specific situations on request, including on resolution of issues and follow up.

Finance

- Ensure that financial transactions/operations (including contact with financial institutions, usage of certain currency, segregation of funds) are in line with economic trade sanctions regulations, by following approved processes and controls.

Risk

- Risk screening tools – upfront and ongoing checks.

9. Employee Responsibility

9.1 You have the obligation to read and follow this Policy, to understand and identify any red flags (including, but not limited to, those identified in paragraph 7.3 above) that may arise in your business activities and to escalate potential compliance concerns related to sanctions to the Legal Department. You should not take any actions prior to receiving advice and/or instructions.

9.2 Sanctions information is included in the broader annual financial crime training which must be completed on an annual basis.

10. Non-compliance

10.1Any Alpha employee or contractor, who violates this Policy may be subject to appropriate disciplinary action, independently from potential other penalties resulting from their behaviour.

Approved by the Group Co-ordination Committee

Issued: February 2024

Whistleblowing Policy

1. About this policy

1.1 Alpha is committed to conducting our business with honesty and integrity and we expect all staff to maintain high standards. In this policy, "whistleblowing" means the reporting of suspected wrongdoing by Alpha or its employees. Any suspected wrongdoing should be reported as soon as possible.

1.2 This policy covers all employees, consultants, contractors, interns and agency workers.

1.3 The purpose of this policy is:

(a) to **encourage staff to report suspected wrongdoing** as soon as possible;

(b) to provide staff with **guidance as to how to raise those concerns** (see section 4 below);

(c) to **reassure staff that they can raise genuine concerns without fear of reprisals**, even if they turn out to be mistaken (see section 7 below).

1.4 This policy does not form part of any employee's contract of employment, and we may amend it at any time.

1.5 Whistleblowing information is included in the broader annual financial crime training which must be completed on an annual basis.

1.6 The Audit and Risk Committee of the Board of Directors of Alpha Financial Markets Consulting PLC has overall responsibility for the effective operation of this policy and for reviewing the effectiveness of actions taken in response to concerns raised under this policy.

2. Who does this policy apply to?

This policy applies to all persons working for any Alpha Group or on our behalf in any capacity, including employees at all levels, directors, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located

3. What is whistleblowing?

3.1 Whistleblowing is the reporting of suspected wrongdoing or dangers in relation to our activities. This includes (but please note that this is not an exhaustive list):

(a) bribery,

(b) facilitation of tax evasion,

(c) fraud or other criminal activity,

(d) unauthorised disclosure of confidential information (including Alpha's or a client's information),

(e) conduct likely to damage Alpha's reputation,

(f) any breach of legal or professional obligations,

(g) health and safety risks,

(h) the deliberate concealment of any of the above matters.

3.2 A **whistleblower** is a person who raises a genuine concern relating to any of the above. If you have any genuine concerns related to suspected wrongdoing or danger affecting any of our activities (a **whistleblowing concern**) you should report it under this policy.

3.3 Please note: this policy should not be used for complaints relating to your own personal circumstances, such as the way you have been treated at work. In these cases, you should use the Grievance Procedure or Anti-harassment and Bullying Policy as appropriate. Accordingly, following a matter being raised under this policy, we may determine (based on the facts) that it is most appropriate for the matter raised to be addressed under one of these other policies.

3.4 If you are uncertain whether something is within the scope of this policy you should seek advice from one of the Whistleblowing Officers whose contact details are set out at the end of this policy. **Further information in respect of what constitutes whistleblowing is set out in the Appendix to this Policy.**

4. How to raise a concern

4.1 We hope that in many cases you will be able to raise any concerns with your Mentor. However, where you prefer not to raise it with your Mentor for any reason (for example, if your concern relates to your mentor), you should contact one of the Whistleblowing Officers, Matthew Mace, Nora Soos and Eloise Lipkin. Alternatively, you can use the confidential external service, ReportIT. Contact details are at the end of this policy.

4.2 We will arrange a meeting with you as soon as possible to discuss your concern. You may bring a colleague to any meetings under this policy. Your companion must respect the confidentiality of your disclosure and any subsequent investigation.

4.3 While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and in an appropriate way. By using this policy, you can help us to achieve this.

4.4 If you are not satisfied with the way in which your concern has been handled, you may contact the Chairman of the Board of Alpha

Whistleblowing Policy

Financial Markets Consulting PLC. The Chairman's Contact details are set out at the end of this policy.

5. Confidentiality

5.1 We hope that staff will feel able to voice whistleblowing concerns openly under this policy. If you want to raise your concern confidentially, we will make every effort to keep your identity secret and only reveal it where necessary to those involved in investigating your concern.

5.2 We do not encourage staff to make disclosures anonymously, although we will make every effort to investigate anonymous disclosures. You should be aware that proper investigation may be more difficult or impossible if we cannot obtain further information from you.

6. External disclosures

6.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.

6.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. We strongly encourage you to seek advice before reporting a concern to anyone external.

7. Protection and support for whistleblower

7.1 We aim to encourage openness and will support whistleblowers who raise genuine concerns under this policy, even if they turn out to be mistaken.

7.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a genuine concern. If you believe that you have suffered any such treatment, you should inform one of the Whistleblowing Officers.

7.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action.

7.4 However, if we conclude that a whistleblower has made false allegations maliciously, the whistleblower may be subject to disciplinary action.

8. Contacts

Whistleblowing Officers

Matthew Mace – Global Head of Legal and Corporate Affairs

Eloise Lipkin – Global Head of Risk

Nora Soos – Global HR Director

ReportIt

(Independent whistleblowing service)

Scan the QR code or text ALPHAFMC to 63975

North America:

go to www.reportit.com and use code ALPHAFMC

Chairman of the Board Ken Fry

ken.fry@alphafmc.com

Appendix – Explanation of what constitutes Whistleblowing

The information set out below is based on the position under English law. However, most jurisdictions have similar protections for whistleblowers to ensure that they can raise genuine concerns about wrongdoing, without fear of reprisals.

What is Whistleblowing?

"Whistleblowing" is the reporting of information which, in the reasonable belief of the worker making the report, is:

1. **made in the public interest** (see further explanation below); and
2. tends to show one or more of the following types of wrongdoing:

(a) that a criminal offence has been committed, is being committed or is likely to be committed,

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he/she/they is subject,

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur,

(d) that the health or safety of any individual has been, is being or is likely to be endangered,

(e) that the environment has been, is being or is likely to be damaged, or

Whistleblowing Policy

(f) that information tending to show any matter falling within (a) to (e) has been, is being or is likely to be deliberately concealed.

Reasonable belief about wrongdoing

The worker must have a reasonable belief that the information disclosed tends to show one of the types of wrongdoing listed above.

The worker does not have to prove that the facts or allegations disclosed are true. As long as the worker subjectively believes that the relevant wrongdoing has occurred or is likely to occur, and their belief is objectively reasonable, it does not matter that the belief subsequently turns out to be wrong.

Disclosure must be in the "public interest"

The disclosure need only be in the public interest according to the "reasonable belief" of the person making the disclosure.

Workers cannot use whistleblowing as a vehicle for grievances personal to their own employment situation. For example, these concerns should properly be addressed under the Grievance Policy or Anti-Bullying and Harassment policies. However, just because the worker may be concerned with their own self-interest, that does not mean they cannot establish that they reasonably believed their disclosure was also in the public interest.

Factors to be considered in determining whether a disclosure is in the public interest include the following:

– the numbers in the group whose interests the disclosure served; although this is not - in itself

– a determinative factor (and in most cases one or more of the additional factors below will also be needed);

– the nature of the interests affected and the extent to which they are affected by the wrong-doing disclosed – a disclosure affecting a very important interest is more likely to engage the public interest than a disclosure of a trivial nature;

– the nature of the wrongdoing disclosed – for example, a deliberate act of wrongdoing is more likely to meet the test than inadvertent behaviour; and

– the identity of the alleged wrongdoer – a disclosure concerning a more prominent wrongdoer is more likely to serve the public interest.

Amended: April 2025

MNPI Share-dealing policy

1. **Policy statement**

1.1 Alpha conducts all its business in an honest and ethical manner, in compliance with applicable laws, and expects all its staff to do the same.

1.2 We take our legal responsibilities very seriously and wish to ensure that all Alpha staff understand their legal obligations and comply with them.

2. **About this policy**

2.1 The purpose of this policy is to:

(a) set out our responsibilities, and those of Alpha staff, in respect of "material non-public information" (defined below) obtained in the course of Alpha's business activities; and

(b) provide guidance to ensure that Alpha staff comply with applicable legal obligations in respect of such information.

2.2 This policy does not form part of any contract of employment or other contract to provide services, and we may amend it at any time.

3. **Who does this policy apply to?**

This policy applies to all persons working for any Alpha group company in any capacity, including employees at all levels, directors, officers, agency workers, seconded workers, interns and contractors, wherever located. Alpha will maintain an insider list for relevant transactions and people.

4. **Who is responsible for the policy?**

4.1 The Global Co-ordination Committee has overall responsibility for the effective operation of this policy and has delegated responsibility for overseeing its implementation to the Global Head of Legal and Corporate Affairs.

4.2 This policy is reviewed regularly by the Global Head of Legal and Corporate Affairs, the Global Head of Risk and other senior executives.

5. **What is Material Non Public Information?**

5.1 In the course of Alpha's business activities, Alpha staff may become aware of and/or have access to confidential information in respect of third party companies, including clients. Alpha staff must keep such information confidential – in accordance with their employment contract (or other terms of engagement) and the terms of any applicable agreement with that third party.

Alpha staff must also comply with any client specific confidential information and data handling policies and training to which they are subject.

5.2 In some instances, this confidential information may also be **Material Non-Public Information ("MNPI")**, MNPI is a specific type of confidential information in respect of companies whose securities are publicly traded (for example, on the London Stock Exchange or NASDAQ).

The definition of MNPI varies from country to country, but in general terms it is:

- Precise information
- Which has not yet been made public
- Which relates to an issuer of shares/securities
- Which, if made public, would be likely to significantly impact the price of those shares/securities. The information is likely to be considered material if there is a substantial likelihood that a reasonable investor would find it important in making an investment decision, by having significantly altered the total mix of information available.

5.3 It is a general rule of most exchanges and markets where shares/securities are publicly traded, that "material" information (i.e. information which would likely significantly impact the price of those shares/securities) should be released to the market as a whole at the same time, for example, through an announcement made through an approved regulatory news service. This is to ensure that investors have equality of information and that certain individuals who, by virtue of their employment by, or association with, the company, do not have an unfair advantage by being able to use information they possess which is not yet public - for example:

- by buying shares before the announcement of a corporate event (e.g. winning a major contract) which causes the share price to rise significantly: or
- selling shares before the announcement of a corporate event (e.g. the loss of a major contract) which causes the share price to fall sharply.

5.4 Further, in most jurisdictions, including the US, UK and other countries where Alpha has operations, it is **both a civil and a criminal offence** to misuse MNPI to deal in shares (so called "insider dealing").

Insider dealing can result in **not only substantial fines but also imprisonment.** For example, in the UK insider dealing is punishable by up to 10 years' imprisonment and in the US by up to 20 years' imprisonment.

These are personal liabilities – so please ensure that you understand this policy and your obligations.

MNPI Share-dealing policy

What is insider dealing?

Broadly speaking, a person will be guilty of insider dealing if:

- that person possesses information in relation to a company which is not generally available to the market and which, if it were generally available to the market, would be likely to materially affect the price or value of that company's securities (i.e. information that is price sensitive); and

- that person:

o acquires, disposes of or engages in other dealings in securities in the company;

o procures someone else to acquire, dispose of -or engage in other dealings in securities in the company; or

o passes on that information to a third party where that person knows, or ought reasonably to know, that the third party would be likely to acquire, dispose of or engage in other dealings in the securities or procure someone else to do so.

6. Identifying MNPI

6.1 What constitutes MNPI is dependent on the specific circumstances in each case, our internal policy defines these in more detail.

7. What you must not do

7.1 Definitions

"Deal" or **"Dealing"** means buying, selling, exercising rights or options in respect of any securities.

"Securities" comprise shares, debt securities, warrants, depositary receipts, options, futures and contracts for differences.

7.2 You must not disclose MNPI

You must not disclose MNPI which you hold to any other person. This includes, but is not limited to):

- Any Alpha colleagues outside the team working with you on the project to which the information relates, unless the Executive Director responsible for the project has given you permission to disclose it to the specific person.

- Any friends, family or other members of your household.

In this context, you must also be careful not to inadvertently disclose MNPI and so you should follow normal Alpha procedures for handling confidential information including without limitation:

- Not discussing the MNPI in public places, where you may be overheard

- Not leaving your laptop unattended or working in an environment where your screen can be viewed by other people

- Taking extra care to ensure that emails are sent to the correct recipient(s)

- Not leaving documents containing MNPI on your desk or taking hard copies of them out of the office.

7.3 You must not Deal in securities when you are holding MNPI which relates the company issuing them

You must not deal in securities at any time when you are in possession of MNPI in respect of the issuer of those securities.

This includes asking someone to deal in the securities on your behalf or as your nominee or representative.

7.4 You must not encourage others to Deal in securities when you are holding MNPI which relates to the company issuing them

You must not encourage or induce any third party to Deal in securities at any time when you are in possession of MNPI in respect of the issuer of the securities. This would include (but is not limited to):

- your spouse, civil partner, children or other dependents.

- any company which you have an interest in, whether as a director or shareholder.

MNPI Share-dealing policy

7.5 Inclusions and exclusions

7.5.1 This policy applies:

- to any scheme or arrangement where you have the ability to select individual securities and decide whether to buy or sell them;

- to subscription for shares through a rights issue.

7.5.2 This policy does not apply:

- to life policies, unit trusts, mutual funds or pension funds where you are not able to select the individual securities, spot or forward FX, National Savings Certificates, Premium Savings Bonds and other government issued bonds, cash, property or physical assets such as land, antiques or works of art; or

- scrip dividends (i.e. where shares are issued by a company in lieu of payment of a cash dividend)

8. Additional Guidance and Recommendations

8.1 The Alpha group's business is focussed on providing services to companies operating in the financial services sector. As a consequence, almost any company in that sector could become a client and Alpha could come into possession of MNPI in respect of that company.

8.2 You are therefore strongly recommended not to invest directly in securities in publicly listed financial services companies[1]. **This is a recommendation and not a prohibition**. However, this guidance is given because if you invest in a company and subsequently acquire MNPI in respect of it in the course of your activities working for Alpha, you may be prevented from disposing of those securities (for the period before the information becomes public), which may cause financial inconvenience for you.

9. Your responsibilities

9.1 You must ensure that you read, understand and comply with this policy. If you have any questions in respect of the policy, please email: [legal@alphafmc.com].

9.2 You must notify the Global Head of Legal and Corporate Affairs as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur in the future.

[1] Indirect investments (as specified in paragraph 7.5.2, such as unit trusts and mutual funds, for example) where you do not have the ability to select the individual securities, are not subject to this paragraph 8.2.

How to raise a concern

10.1 If you are unsure about the applicability of this policy in any particular situation you should consult the Global Head of Legal and Corporate Affairs.

11. Training and communication

11.1 Training on this policy forms part of the induction process for all individuals who work for us, and regular training will be provided annually. You must attest to training and testing on an annual basis.

12. Breaches of this policy

12.1 Any employee who breaches this policy will face disciplinary action, which could result in dismissal for misconduct or gross misconduct.

Approved by the Global Co-ordination Committee

Issued: February 2024

Conflicts of Interest & Outside Business Interests Policy

Purpose

The purpose of this conflict of interest policy is to protect the interests of Alpha Group. Employees are expected to carry out the duties of their jobs honestly and ethically. This policy refers to any case when an employee has a private interest that contradicts the interests of the Company.

Scope

This conflict of interest policy applies to all employees of Alpha, both prospective and current, as well as independent contractors and persons acting on behalf of the Company. This policy is especially vital to employees who make or influence business decisions and those who have access to the Company's resources, intellectual property and confidential information. Conflicts of interest that fall under this policy may be actual, potential or perceived.

Conflicts of interest could arise from employees receiving material non-public information through outside business interests. Employees are required to declare any outside business interests to Alpha. If an employee's conflict is an outside business interest, please see Appendix A for more information.

Definition & Examples

Conflicts of interest may occur when an employee's private interests lead them to actions, activities or relationships that are harmful to or interfere with the best interests of Alpha. A private interest is anything personal that influences an employee's behaviour, or which might affect their judgment. Private interests can fall into the following categories:

- **Direct**: an interest directly tied to the employee, their family or their career, which includes close personal relationships within the Alpha Group

- **Indirect**: the interest of a group, person or business the employee is or was closely connected to (e.g. a friend of a friend or the employee's previous employer)

- **Financial**: monetary gain or loss

- **Non-financial**: favouritism or prejudice resulting from friendship, animosity, or other personal involvement with another person or group

Employees may seek personal gain through methods including but not limited to:

- Outside work or business activities (e.g. taking sick leave to work at another job, working for a vendor of the company part-time, using connections obtained through Alpha for private purposes)

- Special treatment (e.g. hiring, promoting or working with someone connected to the employee)

- Receiving gifts or kickbacks

- Using company property for personal benefit

- Giving confidential information to competitors or using it to start another business

- Acting in ways that may compromise the company's compliance with law

Procedures

Duty to Disclose

Employees of Alpha should recognize advantages their jobs give them, including:

- Decision-making power

- Confidential information and trade secrets

- Company time

- Access to company resources including money, facilities and supplies

Employees should avoid any situation that could remove their ability to carry out their job ethically and in the best interests of Alpha or where their personal interests might affect their judgment or impartiality. Should a situation like this arise, employees are obligated to disclose the facts of the conflict of interest to the Risk team, after which corrective actions may be taken. Employees are also obligated to report conflicts of interest of which they are aware or suspicious, even if they are not involved.

Employees are required to disclose any romantic, family, or personal relationships with other employees and candidates, especially involving a reporting relationship, such as spouses, partners, or relatives working in the same department or under one another's supervision.

Addressing a Conflict of Interest

In order to avoid a conflict of interest, employees should:

- Disclose their conflict of interest situation to the Risk team

- Await approval or feedback on the declared conflict of interest from the risk team, and any action that is required. In certain situations, this could ultimately lead to the removal from the project, panel or task where the conflict of interests arises

Conflicts of Interest & Outside Business Interests Policy

- Refrain from engaging in outside business activities that conflict with the interests of Alpha

- Refrain from using Alpha property for personal use, including using the Company's devices and platforms to engage in outside business activities

Addressing an Outside Business Interest

In addition, employees are required to disclose any outside business interests so that a determination can

be made as to whether they are considered to present a conflict of interest. Where the potential conflict

is material, the employee may be required to make adjustments to their commitments or dispose of the interest.

Responsibilities of Employees

Every new employee of Alpha will receive a copy of the Conflict of Interest Policy on their first day of work, which will reside within the Corporate Compliance Manual. They are expected to read the policy and will sign an Acknowledgement Form (please see Appendix B) confirming their understanding of the policy's terms.

Employees are expected to understand this policy, and attest to annual Conflicts of Interest training. If an employee seeks guidance on a potential conflict of interest situation or on the interpretation of the policy, they should speak with the Risk team in the first instance.

Responsibilities of Risk Team

The Risk team will:

- Retain records that indicate that employees confirmed they have read and understood the policy

- Give employees access to and guidance on the policy

- Where necessary, book a meeting with an employee who has made a disclosure to discuss the interest, and any adjustments required

- Where there is an outside business interest, the Risk team will review the conflict and issue a formal letter if approved

Disciplinary Action

If Alpha has reasonable cause to believe that an employee has a deliberately not disclosed an actual, potential, or perceived conflict of interest, the Company may choose to conduct an investigation. If the Company determines the failure to disclose was deliberate, disciplinary action up to and including termination may be taken. On behalf of the Alpha Group, the Risk team will attempt to manage and mitigate all conflicts of interest reported wherever possible.

Appendix A: Outside Business Interests

All outside business interests in any other business other than the company/Group have to be pre-approved by the Risk team. To be clear, second homes/holiday rentals etc., are not intended to be captured by this policy.

When considering the impact an outside business interest may have on Alpha, we consider the following factors:

- Time away from Alpha: how will another business interest impact an employee's ability to be present in their Alpha role?

- Financial gain from outside interest: is there significant financial gain from alternative employment?

- Competing with Alpha / Clients – does the second business sell services/products to the same clients as Alpha?

- Reputational risk for Alpha / Clients

Appendix B: Outside Business Interests

Policy Receipt & Acknowledgement Form

I hereby acknowledge and agree:

1. That I have received and read a copy of the Corporate Manual Policy and that I understand and agree to abide by this policy.

2. That I will comply with the rules and regulations outlined in the Conflicts of Interest and Outside Business Interests policy, as a condition of my employment at Alpha.

Employee Name (Print):

____

Employee Signature:

____

Date: ____________________

Conflicts of Interest & Outside Business Interests Policy

Appendix C: Declaration Form: Conflicts of Interest/Outside interest

Declaration Form

Employee Name (Print):

____

[Please delete as appropriate]

I am declaring a conflict of interest

I am declaring an outside business interest

Description: (please supply all details surrounding the conflict of interest or outside business interest, including all of the following criteria):

- *Time away from Alpha*
- *Financial gain from outside interest*
- *Competing with Alpha / Clients*
- *Reputational risk for Alpha / Clients*
- *Are any other Alpha employees or Alpha clients involved? If so, who/how?*

Employee Signature:

____

Date: ____________________

PLEASE NOTE

This is not approved until you have had written confirmation from the Global Head of Risk or the Global Head of Legal and Corporate Affairs.

Issued: July 2023

Amended: July 2025

Modern Slavery Statement

Modern Slavery represents an international problem that transcends age, gender and race. People end up trapped in modern slavery because they are vulnerable to being tricked, trapped and exploited, often as a result of poverty and exclusion. It is these external circumstances that push people into taking risky decisions in search of opportunities to provide for their families or are simply pushed into jobs in exploitative conditions. Modern Slavery is a collective term used to describe things like human trafficking, forced or bonded labour, slavery of children, and forced or early marriage. The Modern Slavery Act makes significant steps towards preventing Modern Slavery in organisations and their supply chains. This statement describes the policies and procedures that Alpha Financial Markets Consulting Group (Alpha) has in place throughout our business, supply and procurement chains to combat slavery and exploitation. It has been made in accordance with section 54(1) of the Modern Slavery Act 2015 and constitutes our statement for the financial year ending 31st March 2025.

Alpha Financial Markets Consulting is a leading global consultancy to the financial services industry, with 1,230 employees across North America, UK and MENA, Europe and APAC.

While Alpha, as a professional services provider, does not operate in an industry where Modern Slavery and Human Trafficking is prevalent, nonetheless, we are dedicated to conducting business at the highest standard and expect all employees to make decisions based on the business's core values of integrity, accountability and responsibility.

To this effect and to fulfil our obligations under the Modern Slavery Act, Alpha has developed dedicated processes for identifying and preventing human rights abuses.

Assessing Risk in Supply Chains:

Our suppliers are in the areas of professional services, commercial real estate, staff benefits and healthcare, facilities management, office equipment and computer hardware and software. All our suppliers are expected to implement a zero-tolerance approach to Modern Slavery, and we pride ourselves on promoting ethical and sustainable business practices. All enquiries surrounding Modern Slavery form part of our ongoing supplier due diligence processes.

From an operational perspective, our teams aim to include ESG criteria in their enquiry process, which would include sustainability checks, adequate people and social policies, and their impact on the wider business. Within Alpha's operational functions, there are defined responsibilities and activities to ensure our business practices are sustainable, considering our long-term impacts and addressing the needs of different stakeholders. This includes a dedicated responsible business manager. We monitor our progress against industry best practice on a periodic basis, and communicate to our investors, employees, clients, and suppliers, who are all key stakeholders of the Alpha business.

Ensuring Fair Compensation and Appropriate Recruitment Procedures:

All Alpha's direct employees are offered competitive salaries based on their roles within a professional services firm, alongside a cash bonus or profit share scheme and other benefits. Employee packages are reviewed at least annually, taking into account market information about similar roles, so that we can continue to attract and retain high-calibre staff. This process also ensures that our packages are a fair reflection of the roles that people are performing and contributions they make. When Alpha uses external providers to assist with recruitment processes, these will always be recommended and reputable recruitment agencies.

Living Wage:

Alpha became an accredited Living Wage employer as of 29th January 2018. The Living Wage is calculated according to real living costs and represents Alpha's continued commitment to remunerating its employees and support staff fairly. Alpha continues to have regular dialogue with its contractors employing staff working across the Alpha London with regard to their levels of staff remuneration.

Employee Training and Awareness:

All Alpha policies are available for staff to access on our HR portal, and we continue to roll out ad-hoc training where required. Globally, employees receive training focused on fostering respect and inclusion in the workplace. This training provides an action toolkit and identifies the necessary support channels if an employee is witness to any incidents that may need intervention or reporting.

How to Report Suspicions of Slavery:

Alpha remains committed to protecting whistle-blowers and encourages employees, who suspect wrongdoing of any nature, including that of human rights abuse and slavery, to report this information via the processes outlined in the employee handbook. Alpha measures this area by recording the number of concerns raised and investigated in line with the Modern Slavery and Human Trafficking Policy. There were no cases reported this year. We have also developed an anonymous reporting functionality that allows employees to raise any concerns they may have regarding Modern Slavery and Human Trafficking.

Wellbeing While Working Remotely:

We continue to make efforts to promote the well-being of our staff who are hybrid working.

Alpha recognises how inflation pressures and the wider macroeconomic climate have meant within society some children have not had the same opportunity to learn remotely due to a lack of suitable technology at home.

Modern Slavery Statement

Therefore, in the UK Alpha has partnered with various foundations in order to donate spare laptops to local schools and vulnerable families in need of technology.

How to Report Suspicions of Slavery:

Alpha remains committed to protecting whistle-blowers and encourages employees, who suspect wrongdoing of any nature, including that of human rights abuse and slavery, to report this information via the processes outlined in the employee handbook. Alpha measures this area by recording the number of concerns raised and investigated in line with the Modern Slavery and Human Trafficking Policy. There were no cases reported this year. We also have an anonymous reporting functionality operated by an external provider that allows employees to raise any concerns they may have regarding Modern Slavery and Human Trafficking.

Alpha will review and update this statement annually in line with section 54(1) of the Modern Slavery Act 2015 as well as embedding the review in line with Alpha's wider company roadmap.

Approved by the Board on 17 October 2025 and signed on its behalf by:

Luc Baque, Group Chief Executive Officer

If you have questions or would like further information about Alpha's Modern Slavery Statement, please contact esg@alphafmc.com.

Environment, Social and Governance Policy

At Alpha, dedication to sustainable business practices is integrated across our multi-boutique business organisation and operations, reflecting a commitment to long-term success and positive stakeholder outcomes.

Alongside the Group's internal efforts, Alpha's ESG & Responsible Investment propositions are a core and growing part of the work we do with clients. Our consulting teams actively advise on ESG within the investment community, across the asset and wealth management, alternatives and insurance industries. These teams employ distinct approaches to navigate ESG demands, for example supporting financial services organisations in defining their ESG and responsible investment strategies, in adapting to regulatory changes and leveraging technology and data management approaches in managing ESG commitments.

Purpose

The purpose of this policy is to confirm Alpha's commitment to ESG. It is publicly available, and we expect anyone that we work with to respect our approach.

Alpha's ESG policy is supported and implemented through a number of related policies, such as the:

- Environmental policy
- Diversity, Equity and Inclusion policy
- CSR policy

Policy Application

Alpha is committed to a positive policy of embedding responsibility across the Group. As such, this policy applies to all offices, all business areas, all levels from graduate to the CEO, and at all times.

The Group CEO is ultimately responsible for ESG matters at Alpha and the ESG policy.

Overview of Commitment and Approach

Alpha aims for long-term growth and success, relying on maintaining an excellent reputation and delivering results for clients and other stakeholders. We recognise the importance of setting and delivering on the right ESG priorities, as a fundamental part of our future success.

We have conducted a full materiality assessment, to identify the range of topics that are important to Alpha's stakeholders, to assess where Alpha can make the most impact and to refine our roadmap of ESG activities. The first materiality assessment was conducted in 2023; it will be maintained and refreshed from time to time.

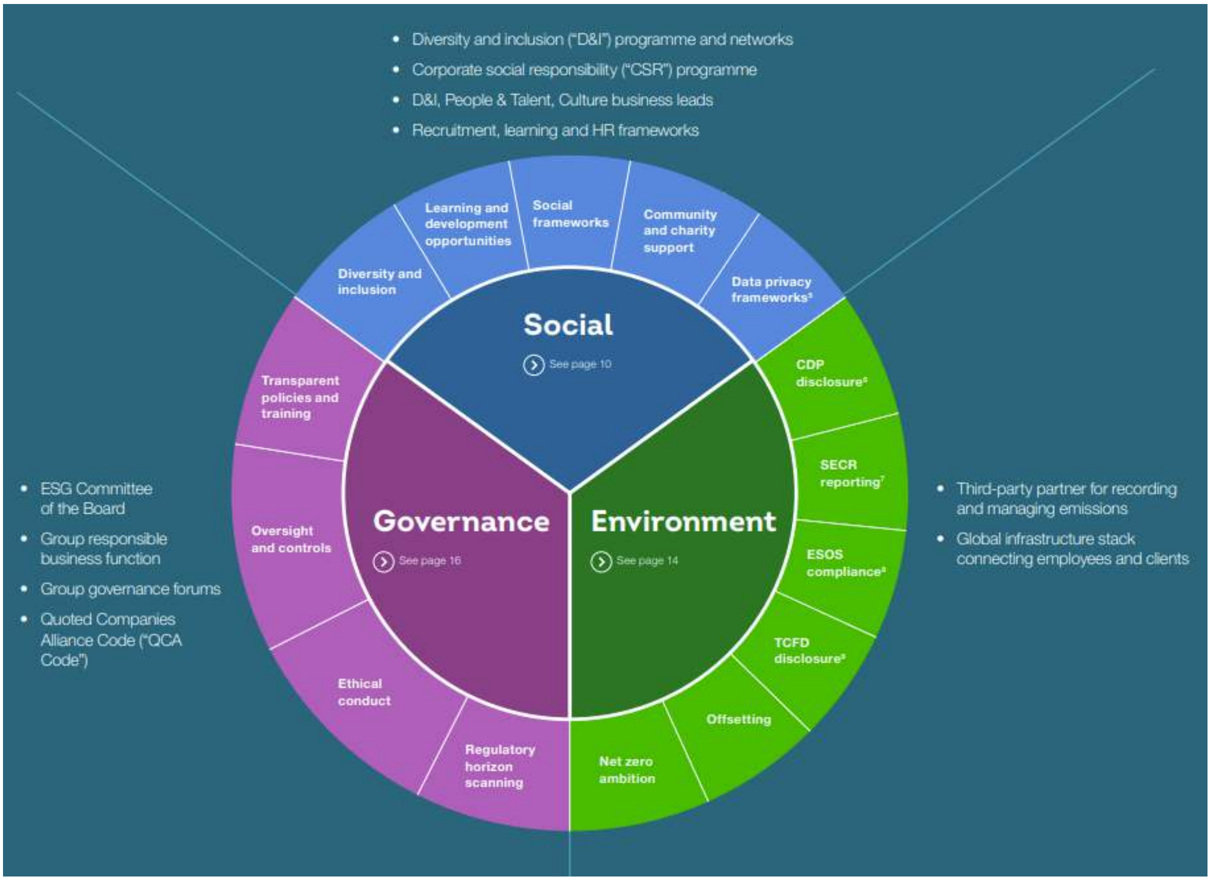
Alpha considers its key stakeholders to be its employees, clients and the communities in which it operates. We also recognise other stakeholder groups including industry bodies and industry partners with whom we may work. Ensuring that we engage effectively with these stakeholders strengthens Alpha's ESG vision and decision making.

We apply a number of different assessment factors in considering the topics that our stakeholders value:

1	2	3
What is the right thing to do?	**What is materially important to our stakeholders?**	**What must we do from a regulatory perspective?**
Alpha's culture is based on integrity, fairness, meritocracy and giving everyone the opportunity to feel they have a part to play in our success. We are socially and ethically responsible, and hold ourselves to the highest standards of transparency, honesty, and personal integrity.	Sustainability is high on the agenda for investors and rating agencies, clients, employees and candidates. ESG and sustainable investment are top strategic priorities for our clients, and many organisations in our ecosystem are under increasing levels of scrutiny.	Across much of the world, ESG management and reporting is shifting quickly from a voluntary to a mandatory activity. As well as meeting prevailing legal and regulatory requirements, we aim to stay ahead of emerging requirements, and to be aware of the risks and opportunities that they present.
Doing the right thing matters to Alpha	**We consider where change is most needed, and where we can make the most impact**	**Regulatory integrity and the adoption of relevant process and governance is essential**

There are three core pillars of Alpha's ESG roadmap, including the most relevant and important focuses for each of the ESG pillars. Our policy includes maintaining an understanding our stakeholder priorities and we will make changes to our pillars as appropriate:

Environment, Social and Governance Policy



Please see the following policies for further details on these priority areas:

- Environmental policy
- Equity, Diversity and Inclusion policy
- CSR policy

These separate policies contained within our Corporate Compliance Manual enable us to provide further details on the varied work happening across the Group in each key area, to ensure clarity and to ensure that nuance is captured across our ESG agenda, whilst providing a high-level view within this policy.

Delivering Our Priorities

Alpha's responsible business function supports the Group in ensuring that we anticipate and address ESG demands. As well as responding to emerging regulatory requirements, the function was formed to support the definition and delivery of Alpha's ESG roadmap, as well as the Group's ongoing commitment to evaluating and progressing its sustainability agenda.

A strong culture of ESG awareness and engagement exists at all levels of the organisation. The responsible business function forms part of a broad, global structure that ensures ESG priorities are identified, safeguarded and progressed.

Environment, Social and Governance Policy

Integration with Risk Management Framework

Alpha's risk management framework combines clear governance, robust processes and controls, and a strong culture of risk awareness among all employees. Climate-related risks and opportunities are identified, assessed, and managed within the Group's existing framework, taking both a top-down and bottom-up approach.

Appendix 1: ESG Certifications and Accreditations

Alpha will comply with the certain voluntary certifications and accreditations as part of our ESG strategy. This aids in the development of policy and processes, including confirming we are conforming to industry standards. These frameworks run alongside mandatory reporting such as SECR, TCFD (see Environmental policy), and Gender Pay Gap reporting for in-scope entities (see Diversity, Equity and Inclusion policy).

The certifications and accreditations are reviewed on an ongoing basis and may be changed. The following are currently applied:

United Nations Global Compact: We are proud to be a member of the United Nations Global Compact, an initiative for global corporations to commit to responsible business practices in human rights, labour, the environment, and corruption.

SASB: The mission of the Sustainability Accounting Standards Board ("SASB") is to develop and disseminate sustainability accounting standards that help corporations disclose material, decision-useful information to investors. We are supportive of the SASB framework as it allows organisations to provide comparable and consistent ESG-related data. The Group adopted the SASB framework in 2019 and we have reported on our adherence to those standards each year since.

UK Living Wage: As part of our commitment to ensuring our supplier relationships are in line with legislation and best practices, we are a member of the UK Living Wage scheme.

Carbon Disclosure Project (CDP): In the UK, we voluntarily report against the CDP, a global disclosure system for investors, companies, cities, states and regions to manage their environmental impacts. The world's economy looks to CDP as the gold standard of environmental reporting with the richest and most comprehensive dataset on corporate and city action.

EcoVadis: In France, we report to EcoVadis, a globally trusted provider of business sustainability ratings with a network of more than 130,000 rated companies.

Issued: September 2024

Equity, Diversity and Inclusion Policy

Alpha operates in a global market, and, as a provider of professional services, the success of the business is dependent on our people. Our belief is that diverse perspectives and different ways of working will enable us to think smarter, anticipate and meet our clients' and the industry's needs in new ways. This diversity of thought makes us more inclusive, innovative and productive as a company, and a stronger partner for our clients and stakeholders.

We aim to build teams that are diverse, inclusive and engaging, and to establish an environment where all people can thrive. We want to ensure that being successful at Alpha is purely based upon talent, commitment, personal values and effort; consistent with our core values of being meritocratic, sociable and supportive.

Purpose

The purpose of this policy is to confirm Alpha's commitment to providing equal opportunities to all in employment, irrespective of their age, marital status, sexual orientation, gender identity, social class, race, ethnicity, disability, religion or religious beliefs, pregnancy and maternity. This policy covers all Alpha employees, regardless of position or status, and contractors of the company.

Diversity and Inclusion Commitment

- Educate and involve people from all backgrounds to understand and promote all diversity through the organisation;
- Retain Alpha's meritocratic culture of rewarding talent regardless of what makes them unique, whilst continuously challenging our understanding of meritocracy;
- Improve the diversity of both our applicant pool as well as the Alpha team at all levels, and particularly senior levels to ensure representation and diversity of thought. As part of this, we are committed to setting targets to substantiate and hold ourselves to account alongside our aspirations;
- Support external initiatives that raise the profile of underrepresented groups in business;
- Create a positive, inclusive environment for underrepresented groups at Alpha;
- To ensure delivery of an effective DEI agenda, there is engagement globally from a range of business areas, including the regional leadership, global consulting and business operations teams. This agenda is ultimately overseen by the CEO and ESG SteerCo, with the full engagement of the global senior leadership team to define targeted regional initiatives and plans that resonate with local teams.

Policy Application

Alpha is committed to a positive policy of promoting equality of opportunity, providing an inclusive place to work and eliminating any unfair or unlawful discrimination. As such, this policy applies to all offices, all business areas, all levels from graduate to the Group CEO, and at all times.

Monitoring

We collect, monitor and review data across a number of areas including gender, ethnicity, socioeconomic background, sexuality and disability/ long-term health conditions, for employees and job applicants, within the limits of local legislation, to assess that our processes are fair and achieving the aims of this policy. All the information that we collect is held in the strictest confidence, anonymised where possible, and is only used to enable teams to understand their own focus areas and promote DEI agendas. Across the Group, Alpha also runs awareness raising workshops and events to promote these agendas.

We also ask DEI questions within our annual feedback survey, and we further monitor our efforts towards our commitments through our Diversity, Equity and Inclusion programmes. It is important for us to maintain and expand our focus on this topic – therefore, we will continue to review our current processes, practices and policies to see what will help us to make further progress.

Diversity, Equity and Inclusion Programme

Our DEI programme was launched in 2015 to accelerate progress towards this outcome. Activities have included establishing DEI networks, joining key voluntary frameworks such as the Disability Confident Scheme in the UK and the Armed Forces Covenant in North America, building initiatives focused across recruitment and retention, and establishing senior sponsorship for these activities, for example through ManCos.

The Diversity, Equity and Inclusion programme was initially managed and run voluntarily by members of the Alpha team, but since 2022 has been fully overseen by the group-level Responsible Business function and managed by the Group Head of Risk and Responsible Business. Whilst the core Diversity, Equity and Inclusion priorities are overseen centrally, there is a collaborative approach with the global business teams to define and incorporate regional differences.

The programme currently focuses on six key areas of DEI: Social Mobility; Ethnic & Cultural Diversity; Gender Equality; Wellbeing; Pride; and Disability Confidence. We have formalised our approach to diversity, equity, and inclusion and commit to regularly reviewing and evolving our strategy to hold ourselves to account. Our priorities are to:

Equity, Diversity and Inclusion Policy

- Ensure diverse groups are attracted to and encouraged to succeed throughout their Alpha career

- Do what we can to increase the diversity of our workforce and maintain an inclusive and supportive culture, which includes setting Group-wide diversity targets to ensure we are accountable against tangible ambitions. In 2024, we set our first diversity target, for 25% of our senior leadership team to be women or nonbinary by 2029, in recognition of the importance of senior diversity, and in recognition of our belief that workplaces should be inclusive of all gender identities, which our action plans reflect

- Embed our mission and goals into our company growth plans – which focus on being social, supportive and market leaders in our field

- Ensure that the strength of our diversity is transparently communicated to the outside world.

We are committed to hearing the voices of our employees and encourage team members to provide feedback on this topic at any point in time, should they wish to. DEI is fundamental to the ongoing success of the Alpha team.

Issued: January 2019

Amended: March 2025

Environmental Policy

Context to our Environmental Policy

Alpha FMC strives for excellent operational management to mitigate climate-related risks, enhance efficiency, and deliver the highest quality of service.

Alpha FMC has been diligently monitoring its top-level environmental performance for several years, accompanied by offsetting initiatives. We started making disclosures in our 2019 Annual Report and have been offsetting our unavoidable greenhouse gas emissions globally since FY 20 through recognised and certified offsetting projects. Our annual emissions are disclosed through the SECR statement in our Annual Report, and gradual increases year on year due to business expansion.

We are committed to enhancing our data collection and analysis methodologies to create a solid baseline our 2050 deadline to net zero, a key focus of our ESG roadmap. Our environmental policy emphasises reducing emissions over offsetting, prioritising renewable energy, and implementing various energy efficiency and recycling initiatives. We are also now preparing TCFD and ESOS reporting and aim to refine our carbon reduction plans and communicate our net-zero ambitions further in the short-term.

Alpha's approach to Environmental obligations

Alpha's approach to managing environmental factors is underpinned by the following key considerations.

1. Business Growth Strategy

Alpha FMC has an ambitious business expansion strategy, and integrating environmental considerations is core to ensuring that growth is sustainable and successful over the long term. To this end, climate risk and understanding environmental impacts are embedded into Alpha's business management and decision-making processes.

Alpha's approach includes relevant assessments through thorough due diligence in supply chain management and Alpha's acquisition and integration framework.

Alpha also consider both operational and capital expenditures relating to employing sustainable practices and infrastructure in the context of financial planning. For operational expenditure, this encompasses considering Alpha's focus on sustainable practices in energy consumption, waste management and procurement. For capital expenditure, this includes assessment of relevant investment in infrastructure and new projects, such as employing more energy-efficient technologies and reducing overall carbon footprint

2. Benchmarking Alongside Peers (Market Sentiment)

To maintain our leadership in sustainability, We continuously benchmark our environmental performance against peers, utilising analysis and third-party insights.

This ensures we remain at the forefront of market trends and public sentiment, maintaining our commitment to environmental excellence. expectations.

3. Helping Clients Deliver Sustainable Outcomes

Our dedicated ESG practices assist clients in achieving sustainable outcomes through various initiatives:

TCFD Benchmarking: Analysing firm-level and product-level disclosures in line with FCA climate-related requirements.

Webinars and Roundtables: Hosting sessions on regulatory topics such as SDR and CSRD, showcasing sustainable investment FinTech advancements.

Wealth Management Collaboration: Partnering with industry bodies like PIMFA to address sustainability regulations and their impact.

Thought Leadership: Publishing articles on ESG data integration, biodiversity, sustainability risk, anti-greenwashing, and regulatory updates.

4. Regulation

Since 2019, we have reported our emissions performance, with our inaugural CDP disclosure in 2021.

We are fully compliant with environmental regulations, including SECR, TCFD, and ESOS standards. In France we have also obtained an Eco Vadis Silver rating. Our commitment includes transparent reporting and periodic updates on our emissions data.

We also align our sustainability promises with CDP standards, conducting retrospective reviews to ensure we meet our commitments.

5. Sustainable Supply Chain

We expect all suppliers to adhere to our Supplier Code of Conduct, which sets key principes for environmental and social policies, this due-diligence is also built into our mergers and acquisitions framework. We prioritise greener options and allocate spend to verified offsets, supporting charities and initiatives aligned with Alpha's cultural values.

Environmental Policy

Our partnership with Normative.io highlights our commitment to understanding and reducing our environmental impact. We also use Chubb's leading climate risk management system for real-time assessment and analysis of climate-related risks across our operational geographies.

Sustainability Framework

1. Climate Priorities

We use our climate priorities to inform which environmental topics are most material to Alpha. Utilising both mandatory and voluntary reporting plus peer benchmarking and Alpha's own Environmental Policy, we remain agile to ensure we have the right focus at the right time.

2. Environment Context

Alpha have ESG embedded into the work, culture and values of the Group.

3. Defining Engagement and Assessing Opportunities

Alpha continually assess environmental opportunities using our regulatory drivers such as TCFD taking into account scenario analysis and business growth. This is published in our corporate reporting.

4. Enabling Clients to Achieve their ESG Priorities

We regularly review our climate priorities, identify trends and respond with actions that allow continuous improvement and development through systematic horizon scanning and ongoing assessments of external markets events.

5. Climate Reporting

We provide assurance that climate topics are managed, reported and we ensure full compliance of all regulatory disclosures. Beyond this, we also publish a standalone Sustainability Report every year detailing our progress.

6. Governance

We govern our Environmental priorities through executive oversight and responsibilities covering all business areas.

Process

Alpha FMC is dedicated to a program of continuous improvement in environmental sustainability. We are committed to setting specific, measurable targets, tracking our progress, and sharing our achievements with stakeholders. This process ensures that our efforts in sustainability are transparent, accountable, and aligned with our broader business goals.

Governance and Reporting

Our Environmental Sustainability Performance is rigorously monitored and reported annually through a comprehensive framework and corporate reporting. To maintain transparency and credibility, we employ third-party audits to provide limited assurance on our environmental data and the methodologies used. This ensures that our claims, such as our commitment to carbon neutrality, are robust and verifiable. Additionally, every employee at Alpha FMC is responsible for adhering to our Environmental Policy, and we actively engage with our suppliers to support their alignment with our sustainability goals.

Review

This Environmental Policy is reviewed annually unless there is are new regulations or large business changes that will impact the environmental agenda.

Issued: June 2024

Supplier Code of Conduct

Alpha Group is focusing on co-creating a sustainable future. As a leading global consulting firm in asset management, wealth management, and insurance, we recognise our responsibility to build a better world. Sustainability is no longer optional; it is essential to our collective survival. Our partners and suppliers play a crucial role in achieving our sustainability goals. This Supplier Code of Conduct reflects the principles and expectations that guide our relationships. Together, we can ensure that our operations positively contribute to society and the environment.

We Need to Act Now

The impact of climate change is among the most significant challenges we face. Our suppliers are vital collaborators in this mission, and we call on you to take meaningful action. Through shared effort, we can preserve the ambitions and aspirations of future generations.

1. Commitment to Sustainability

Alpha Group prioritises environmental stewardship and expects suppliers to:

- Disclose annual Scope 1, 2, and 3 greenhouse gas emissions.
- Develop and execute science-based carbon reduction plans.
- Transition to renewable energy where feasible.
- Commit to achieving carbon neutrality through verifiable offset mechanisms.

2. Regulatory and Ethical Compliance

Suppliers must adhere to applicable laws, regulations, and best practices. Key expectations include:

- Upholding international human rights standards, including protections against modern slavery.
- Maintaining robust data governance frameworks and compliance with ISO standards or equivalent.
- Ensuring transparency in financial practices and corporate governance.

3. Social Responsibility

Alpha Group values equitable and inclusive partnerships. We require suppliers to:

- Promote diversity, equity, and inclusion (DEI).
- Promote disability confidence.
- Ensure health and safety standards for all workers.
- Provide clear grievance mechanisms to address workplace issues.
- Actively combat forced and child labour.

4. Professional Integrity

Suppliers must demonstrate integrity and avoid behaviours that jeopardise trust. This includes:

- Avoiding legal and regulatory violations.
- Protecting against cyber risks and maintaining high data security standards.
- Delivering high-quality and ethically sourced goods and services.

5. Transparency and Risk Management

Effective risk management and transparency are essential to sustainable operations. We expect:

- Disclosure of ESG policies and progress.
- Implementation of climate-related risk management frameworks.
- Regular collaboration with Alpha Group to align sustainability objectives.

Collaboration and Continuous Improvement

Sustainability is a continuous journey, and we are committed to supporting our suppliers every step of the way. To help our partners meet shared goals, Alpha Group provides valuable resources and knowledge designed to bolster sustainability ambitions. Additionally, we offer training and opportunities to build capacity for ESG initiatives, ensuring suppliers are well-equipped to meet evolving standards. By fostering an open and transparent dialogue, we aim to overcome challenges together and celebrate shared progress.

Supplier Code of Conduct

We Are On a Journey Together

Collaboration with suppliers is fundamental to achieving our vision of a sustainable future. We invite our partners to set ambitious sustainability targets that align with our collective goals. Adherence to the principles outlined in this Supplier Code of Conduct is essential as we work hand in hand to create a more resilient and sustainable value chain.

Acknowledgment and Acceptance

Collaboration with Alpha Group signifies a commitment to upholding the standards set forth in this Supplier Code of Conduct. By working together, we can build a future defined by sustainability, equity, and integrity.

Issued: April 2023

Updated: March 2025

Supply Chain Due Diligence

With Alpha's position as a leading global consulting firm in the asset and wealth management, insurance and alternative investment industries, we are committed to positively contributing to society and the environment and facilitating a world of possibilities for future generations.

Our partners and suppliers are integral to our business and delivering the best service to our clients; they are also critical enablers of the sustainability commitments we make.

Definition of Critical Suppliers

As a global consultancy group operating in multiple countries, we take a risk-based approach to our processes and apply our due diligence framework to our most critical suppliers and business partners. As a financial consultancy, critical suppliers are those whose goods, services, or operations are indispensable to delivering high-quality advisory services, ensuring regulatory compliance, and maintaining the infrastructure necessary for business continuity. Key categories include technology providers for secure data handling, office space providers for client and team engagements, and accounting services for financial accuracy and reporting.

The criticality of a supplier is evaluated based on their direct impact on Alpha's daily functions and strategic outcomes. This assessment is conducted within the framework of supplier relationships and information security standards such as ISO27001:2022 Annex A 5.22 and ISO27036, ensuring alignment with Alpha's principles and resilience standards.

The criticality of a supplier will be assessed annually, or where there is a significant event or business change impacting a process and/or part of our supply chain.

Governance

The Risk, Responsible Business, and Infosec teams will use publicly available data to collect the relevant data points for our main suppliers and business partners to ensure that they align to core Alpha priorities. Those that do not will be contacted for further information. Where appropriate, companies will be flagged to the relevant Business Lead that manages the relationship.

Where necessary, escalations will be addressed by the ESG SteerCo which consists of the Group Head of Risk and Responsible Business, Group COO, Group CEO and Group Managing Director.

Team members should save down evidence of checks in relevant risk Box folder. N.B. we only require supporting evidence where there is a negative outcome for the search, i.e., adverse media or regulatory fine.

Priority area	Compliance check	Frequency
Commitment to Sustainability	1. Suppliers must disclose their annual scope 1, 2 and 3 emissions. 2. Evidence for carbon reduction plans and adoption of renewable energy solutions, where possible	1.Annual check 2.Annual check
Regulatory and Ethical Compliance	1. Adherence to regulatory requirements 2. Acceptance of Alpha's Supplier code of conduct 3. Modern slavery protections	1.Ongoing, adverse media scans and reg investigations 2.Upfront, at time of onboarding 3.Upfront, at time of onboarding
Social Responsibility	1. Policies for Health and safety standards, clear grievance and whistleblowing procedures 2. evidence that a company meaningfully supports diversity, equity, and inclusion (DEI) initiatives,	1.Annual check 2.Annual check
Professional Integrity	1. Utmost professional integrity standards; not be subject to legal or regulatory fines, major cyber incidents or data breaches	1. Annual check, ongoing awareness
Transparency and Risk Management	1. Evidence of transparent corporate policies and a strong governance framework are critical	1. Annual check for public documentation, ongoing awareness for key person departures

Issued: April 2023

Updated: March 2025

Information Security Policy

1. Document Control

This Policy needs to be formally reviewed on an annual basis, as a minimum, or if required changes are identified to address one or more of the following:

• A change in business activities, which will or could possibly affect the current operation of the Alpha FMC Information Security Management programme.

• A change in the way Alpha FMC manages or operates its information assets and/or their supporting assets.

• An identified shortcoming in the effectiveness of this Policy, for example as a result of a reported information security incident or an audit finding.

2. Policy Objectives

To direct the design, implementation and management of an effective Information Security Management System (ISMS), which ensures that Alpha FMC's information assets are properly identified and recorded and afforded suitable protection at all times.

Business Units not in compliance with one or more sections of this Policy are required to evaluate and document the exception(s) and propose timelines to become compliant and make a request to the Global Information Technology Team for approval of the exception based on the risk and exposure at the local and enterprise level, including business justification and compensating controls. Exceptions must be approved by the Global Information Technology Team and to the extent required by the Group Coordination Committee and may be subject to periodic review to ensure the exception and associated business justification continue to be relevant and appropriate.

To ensure the confidentiality, integrity and availability of Alpha FMC's information assets, and supporting assets (including information systems) as defined within an Inventory of Assets.

To ensure that all vulnerabilities, threats and risks to information assets and supporting assets are formally identified, understood, assessed and controlled.

To ensure that Alpha FMC's employees, contractors and third party users comply with this Information Security Policy, and all other ISMS documentation, through the provision of effective information security training, awareness and ongoing monitoring activities.

To ensure that Alpha FMC can maintain full compliance with all applicable legislation, regulations and contractual requirements (e.g. the EU General Data Protection Regulation), and any supporting management system certifications (e.g. ISO/IEC 27001:2013).

To ensure that the security needs and expectations of "interested parties" are obtained, recorded and addressed, for example those of customers, stakeholders, personnel, regulators and statutory authorities.

3. Policy Scope

This policy applies to all persons working for any Alpha Group or on our behalf in any capacity, including employees at all levels, directors, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located

Alpha FMC's Information Security Policy shall include the following:

3.1 Information Assets

All information assets (data) either owned by Alpha FMC or entrusted to Alpha FMC by a client under an agreement which specifically details Alpha FMC's responsibility for that data, and including:

• Information assets held, processed or stored on Alpha FMC information processing facilities;

• Information assets held, processed or stored at approved off-site information processing facilities.

3.2 Disciplinary Sanctions

It is Alpha FMC's duty to sanction any workforce member in violation of security privacy and security policies and procedures, whether the violation was intentional or unintentional. Formal Disciplinary procedures are outlined on the Employee Handbook.

3.2 Supporting Assets

All supporting assets (non-data) which by direct or indirect association are an integral part of ensuring the confidentiality, integrity or availability of the information assets described, including:

• Premises (including offices, factories, data centres, storage facilities, recovery sites etc.);

• Hardware (including servers, network infrastructure, laptop computers, desktop

computers, storage infrastructure and mobile devices);

• Software (including operating systems, commercially available software applications and

software applications developed internally by Alpha FMC);

• Alpha FMC personnel (including permanent, temporary, full-time and part-time employees, authorised contractors and any third-party users of information systems);

• Alpha FMC shall require all Assets to be appropriately classified or identified with sensitivity classifications. "Sensitive Information" shall be referred to any Alpha FMC trade secrets, intellectual property, and other assets owned or licensed by Alpha FMC accordance with applicable laws and Alpha FMC Policies, as well as personally identifiable information and other confidential or proprietary information of Alpha FMC, our employees, customers, vendors and partners. Systems holding customer data, personally identifiable information (PII) and electronic personal health information (ePHI) data shall be treated as sensitive information and be secured throughout their life cycle accordingly.

3.3 Documentation and Records

All policies, processes, procedures, work instructions and records related to the management, use, control and disposal of the information assets and their supporting assets detailed above.

4. Policy Statements

4.1 General Statements

Alpha FMC shall be committed to the protection of the information assets and supporting assets as defined within the Scope of this Policy.

Alpha FMC has created its Information Security Management System (ISMS) to align with best practice guidance from within international management system frameworks and NIST cybersecurity guidelines.

To effectively manage and deliver its ISMS, Alpha FMC shall:

Inventory of Assets and/or Services

Define and maintain an Inventory of Assets (and/or Services), including all information assets and supporting assets as defined within Section 3.0 of this Policy. The Inventory of Assets shall detail a named owner for each asset or service, who shall fully understand their responsibilities for the protection of the asset.

Access Control Policy

Ensure that an Access Control Policy is in place to protect all Alpha FMC networks, information systems and information assets from any unauthorised access. Legitimate remote access shall only be granted in accordance with the policy to bona-fide personnel, contractors and third party users, and only applies to access from Alpha FMC approved devices. Remote connections shall be used strictly in accordance with the **Acceptable Use Policy**. Remote access shall be regularly reviewed and any connections that are no longer required shall be removed immediately.

Ensure that all information assets, and their supporting assets, are protected so as to ensure their confidentiality, integrity and availability is maintained. Access to information assets and supporting assets shall be in accordance with **Alpha FMC's Access Control Policy**, and be restricted to the minimum required to undertake authorised business activities, and Alpha FMC has adopted the principle that "access is forbidden unless it has been specifically and formally pre-authorised".

Alpha FMC's access management is controlled, audited and evidenced as part of the **Alpha FMC Joiners, Movers, Leavers (JML) Policy.**

Information Classification and Handling

Ensure that all information assets shall be classified and handled in accordance with the Alpha FMC Data Privacy Policy which details how information assets shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required.

System and Network Device Security

Assets shall be protected from physical and environmental threats to prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Assets shall be installed or stored (including if only temporarily stored) in areas that reduce the risk of environmental threats and hazards, and unauthorized access.

Assets shall be protected from power failures and other disruptions caused by failures in supporting utilities. Supporting utilities include electricity, water supply, fire prevention, heating, ventilation, and air conditioning.

Backup Procedures and Off-Site Storage

Formal backup procedures shall be developed and implemented to maintain integrity and availability of Alpha FMC Assets. Backups shall be retained in accordance to the data classification guidelines.

Backup of Assets should be performed on a scheduled basis to meet Divisional and/or Business Unit requirements and to allow for recovery to the last known integrity point.

Backup media containing Sensitive Information should be encrypted unless encryption is not allowed under applicable law. Encryption keys should be secured as listed in the encryption standards and should be available to decrypt the information for as long as the retention standards require.

Backup media should be stored in a secure, off-site storage location that is sufficiently distant from the location of the backed-up Systems to ensure that back-up and recovery objectives can be met.

Information Security Policy

Secure transportation of backup media to off-site storage locations should be provided.

System Planning and Acceptance

The planning of new Assets should ensure that logical and physical security requirements are included in the design. Production acceptance should include these criteria:

- Updated standards and operating procedures to include the new Asset, including startup, shutdown, restart, failover, recovery, restore, and business continuity procedures;

- Validate security and adherence to Information Security & data classification handling;

- User training is complete;

- Development-to-production migration procedures exist and have been tested. These procedures include rollback in case of failure;

- Infrastructure configuration changes are completed and documented (including appropriate diagrams).

Acceptable Use

Ensure that all personnel, contractors and third party users comply with the **Alpha FMC Acceptable Use Policy** which details how information assets and their supporting assets should be used in an acceptable manner and in accordance with all ISMS related policies and processes. This policy shall detail the acceptable methods of use of information processing systems, networks (including, for example, the internet and telephone systems) and other resources within the Scope of this Policy.

Information Security Incidents

Provide a mechanism for the prompt identification, reporting, investigation and closure of information security incidents to Alpha FMC, in accordance with the **Security and Breach Management section** of the **Alpha FMC Data Protection Policy**, and to fully analyse reported incidents to identify the root cause of issues and take advantage of any improvement opportunities which may have been identified.

Business Continuity Management

Ensure that information security is a key consideration within Business Continuity Management, so that the security of Alpha FMC information assets is not compromised even when faced with a wide variety of unplanned business interruptions.

Alpha leverage a wholly cloud and Software as-a-Service based Infrastructure stack within resilient, High Availability data-centres. There is no on-premise business critical infrastructure hosted by Alpha FMC, allowing our consulting workforce to continue working remotely and offsite on a regular basis.

Secure Development

Ensure that any software applications are developed and managed in accordance with the **Alpha FMC Secure Development Policy**, such that Alpha FMC and customer data is not subject to vulnerabilities and threats whilst being processed by such applications as a result of insufficient development personnel knowledge, poor development practices or ineffective security testing.

Information Security Training

Develop an annual training and education programme, in accordance with the **Alpha FMC Information Security Training Policy**, which shall be mandatory for all Alpha FMC employees, contractors and third party users, which details and tests their individual responsibilities to fully adhere to the requirements of the ISMS policies, processes and work instructions defined within Section 3.0 of this Policy.

Management, Monitoring and Review

Continually monitor, review and improve the Alpha FMC ISMS, by undertaking regular reviews, internal audits and other related activities, and taking prompt corrective actions and implementing improvement opportunities in response to the findings of these activities.

Technical assessments and reviews such as external and internal penetration testing and vulnerability scanning will be carried out annually at minimum by an independent accredited security partner. Any findings or issues identified through these exercises will be promptly prioritised and addressed by the Global IT Function.

Legislative Compliance

Ensure that, at all times, its Information Security Management System shall follow guidelines and best practice from within the following UK legislation and regulations, including but not limited to:

- The Data Protection Act 2018/GDPR;
- Human Rights Act 1998;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Companies Act 1985;
- Regulation of Investigatory Powers Act 2000;
- Electronic Communications Act 2000;

Information Security Policy

• Freedom of Information Act 2000;

• Waste Electrical and Electronic Equipment Directive (WEEE) 2003.

5. Responsibilities

5.1 Employees, Contractors and Third Party Users

Within Alpha FMC, all employees, contractors and third party users shall understand their role in ensuring the security of information assets (and their supporting assets) in accordance with the Information Security Training Policy as detailed in Section 4.0.

All employees and individuals who perform work for Alpha FMC and who have access to the Information Systems, will be informed of their responsibilities for adhering to applicable Alpha FMC policies. Those responsibilities shall include, but not be limited to, the handling of Critical Assets created as a result of, or in the course of, employment or the engagement of work on behalf of the organization. Those responsibilities shall extend to outside the Alpha FMC office location where the individual may work (i.e. home offices) and outside normal working hours.

There are, however, additional responsibilities defined in order that the ISMS shall operate efficiently and aligns with best practice. These are detailed below.

5.2 Global IT and Infrastructure SteerCo

• The Global IT and Infrastructure Steerco shall be responsible for the following activities within the Alpha FMC ISMS;

• Agreeing the business need for the Information Security programme, and communicating their ongoing commitment to it;

• Reviewing and signing off this Information Security Policy;

• Setting and reviewing Alpha FMC's Information Security Objectives;

• Assigning appropriate resources necessary to manage and operate the ISMS effectively

• Approving any decisions not to address any unacceptable residual risks, where identified;

• Having ultimate responsibility for actions related to information security incidents/breaches;

• Overseeing any disciplinary action resulting from information security incidents/breaches;

• Overseeing any findings and remedial activities resulting from an internal audit.

5.3 Global IT Function

The Global IT Function shall have functional responsibility for Information Security, and shall be responsible for the daily operational tasks of the Information Security function, including:

• Ensuring an appropriate structure of Information Security policies, processes and work instructions;

• Ensuring that appropriate records are created and maintained for all ISMS activities;

• Arranging a programme of risk assessments, risk treatments and internal audit;

• The provision of an appropriate user training and awareness programme for employees;

• Overall management of the information security controls in production processes;

• Overall management and functionality of Alpha FMC's business continuity plan;

• The provision of a user training and awareness programme for suppliers and contractors;

• The design and review of technical security controls, including Alpha FMC networks;

• Undertaking detailed risk assessments on technology asset(s), including the identification of controls and assessing their effectiveness;

• Addressing any unacceptable risks;

• Assisting in the investigation, resolution and closure of any information security incident which directly or indirectly affects the security of technology asset(s);

• Reviewing and authorising the levels of access to technology asset(s) which are granted to others.

5.4 Data Protection Representatives

The Alpha FMC Data Protection Representatives shall be responsible for:

• The Company's compliance with its Data Protection Policy and the European Union General Data Protection Regulation (EU-GDPR);

• The provision of a programme of data protection training and education for all personnel, contractors and authorised third parties;

• Arranging a programme of privacy impact assessments;

• Providing appropriate advice and guidance to Senior Management on data protection matters.

Information Security Policy

5.5 Local Management

Local management teams within Alpha FMC shall be responsible for:

• Ensuring their team members are aware of and remain compliant with all information security policies, processes and work instructions, and that they receive appropriate training;

• The provision of a user training and awareness programme for applicable third party users;

• Supporting reviews, internal audits and risk assessments within their area of responsibility.

5.6 Compliance

Alpha FMC's Users, and their Assets, should comply with all applicable statutory, regulatory, and contractual security requirements. The Global Information Technology Team will review existing, forthcoming, and updates to existing regulations and legislation to determine its applicability to Alpha FMC.

Alpha FMC will take appropriate steps, in accordance with applicable laws and requirements, to retain the rights to all patentable, copyrightable material, inventions, and other intellectual property as is designated on employment contracts.

Information Retention and Back-up Based on compliance requirements, Alpha FMC will establish information retention standards to ensure that information is retained for its defined retention period regardless of its media format. Sensitive Information should be backed up appropriately and should be restored upon resumption of service following an outage.

Reviews of Global Information Security Policy & Compliance This Policy, Alpha FMC's Assets, and security standards, processes, and guidelines should be reviewed annually or when necessary, by The Group Co-ordination Team and the Global Information Technology Team to ensure compliance with security policies and standards.

Issued: June 2019

Amended: October 2024

Business Continuity Policy

1. Introduction

In accordance with the Business Continuity Institute, the objective of Alpha's business continuity management is to ensure a responsive framework that:

• Enables the identification of potential threats to the Group and the impacts to business operations that those threats, if realised, might cause; and

• Ensures organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities as far as possible.

The purpose of the Business Continuity Policy (the "document", the "policy") is to provide the necessary information and strategies in order for the Alpha Group ("Alpha", the "Group") to execute an appropriate and effective disaster recovery and business continuity plan in the event of a disaster or incident being declared.

1.1. Scope of application

This policy applies to all Alpha FMC entities and employees and will be implemented to fit with the size, location and business profile of each entity. Individual entities may maintain their own business continuity documentation that supplements or explains the practical implementation of the overarching Business Continuity Policy.

This policy applies to all persons working for any Alpha Group or on our behalf in any capacity, including employees at all levels, directors, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners, sponsors, or any other person associated with us, wherever located. This policy will also apply to future group acquisitions.

2. Business Continuity Objectives

2.1. Business objectives

The objectives of Alpha's business continuity policy are to ensure as far as practicable that:

• The initial response to a threat to the Group's normal business activity is as coherent, appropriate and effective as possible in the circumstances;

• The impacts of the threat are controlled to the extent that it is possible and with due consideration of what the Group's executive team (represented by the Group Coordination Committee or "GCC") considers acceptable;

• In recovery to normal business activities, priority is given to maintaining or restoring activities that can be regarded as business critical in the circumstances; and

• Relevant senior executives across the Group are empowered, advised and supported in order to achieve the above, in coordination with others as appropriate.

It is not the objective of the Group's business continuity planning to ensure that, in the worst cases such as extensive illness or absence from work across the Group's staff, full recovery of normal activities can be achieved in a particular timeframe. To ensure such recovery to any specific timeframe would require unachievable resilience measures, such as retaining a significant constant "bench" of non-utilised consultants during normal times.

2.2. Training & Awareness

This policy will be published on globally available channels for all Alpha employees, sub-contractors and associates, as well as Omega branded contractors. Where updates are made to the policy, these will be communicated via the same channels for awareness.

All new joiners will be required to read this policy as part of the induction process and adhere to it. All employees are required to remind themselves of this policy on an annual basis.

3. Business Continuity Policy

3.1. Policy principles

It is the policy of the Alpha Group to:

• Maintain a strategy for responding to and recovering from adverse situations that are in line with an acceptable level of risk, as defined by the GMB

• Ensure that, whenever practical, action is taken to prevent the recurrence of an adverse situation through adopting appropriate risk controls

• Maintain a wholly cloud and SaaS based infrastructure stack with resilient, high availability data centres; allowing staff globally to work remotely and offsite flexibly

• Align to official local guidance whether that may be government, health authority or other office

• Maintain appropriate response strategies underpinned by a clear escalation and communication process

• Maintain employee awareness of the Group's expectations of them during an emergency or business continuity threatening situation

Business Continuity Policy

• Take account of changing business needs and ensure that response plans and business continuity strategies are revised where necessary

• Remain aligned with good industry practice in business continuity management, taking account of the locations, size and business profile of the Group.

3.2. Policy priorities

Business continuity planning Alpha focusses on the following priorities (in no particular order):

• Health and safety of Alpha's employees

• Initial / emergency responses

• Communications, both internally to employees and externally to clients and relevant third parties

• Recovery and continuity of key business activities, primarily Alpha's ability to service its clients

• Recovery from any negative commercial impacts

• Safeguarding of Alpha's assets and reputation.

3.3. Responsibility for business continuity

Responsibility for business continuity is delegated to the Global Operations Director (the "BCP Owner"). This responsibility is cascaded through the Group's management structure where it is assured and overseen by the GCC. The GCC meets regularly during the year and encompasses all the areas in which business-level risk and priorities may arise or apply, including finance, IT & infrastructure, HR, service delivery and business development. The GCC reports to the Board of Directors of the Group.

Responsibility for localised business continuity matters and planning lies with the heads of country and the heads of business operations teams. These individuals may delegate the undertaking and implementation of business continuity measures in their areas to an appropriate member of their staff, who should be at director level (or equivalent).

3.4. Incident reporting

Any business continuity threat or incident should be reported to a member of the GCC. Upon the occurrence and notification of a disruptive event involving wide consequences within and / or across the Group, it may be necessary to escalate the response. The GCC will convene to provide leadership, coordination, communication and decision making during such a disruptive event.

Other employees may be invited to participate in and support this effort as required to ensure appropriate and effective responses, such as heads of country and heads of business operations areas.

Following resolution or recovery, reviews will be coordinated to ensure that learning is captured and there is the opportunity for continuous improvement.

3.5. Service delivery

As a provider of advisory, professional services that reply upon people there is an extent to which the Group can absorb a worst-case disaster event where there is large scale inability to work, even remotely. This extent or limit will vary depending upon the locations, client projects and project roles affected but it is anticipated to be in the region of 15-20% absence. In these circumstances, the Group recognises that it may need to consider delaying or withdrawing from current project work on a case-by-case basis and ensuring consultation with its clients.

The Group's mechanisms for assessing and transferring work where necessary will continue to be managed through local sales & resourcing forums, with the oversight and involvement of the Local Head of Region if required.

4. Business Continuity Planning

4.1. Approach

Business continuity planning comprises the steps to be taken to ensure an organisation can perform its normal business activities in the scenario of a disruptive threat or event. A disruptive event can be internal or external events as listed in, but not limited to, **Appendix 1**.

The Group's approach involves identifying and defining contingency plans for key business activities, personnel and infrastructure. It also includes the disaster recovery planning for natural disasters, accidents and other incidents that may prevent the Group from conducting business in its usual environment(s). Other aspects include training and awareness in mobilisation, recovery and restoration procedures and requirements, collection of contact information and participation in disaster recovery exercises.

Periodic review and maintenance of the information included in recovery plans is essential to preserve the integrity of the business continuity process.

4.2. Remote working

A key component of the Group's ability to operate within, and recover from, a business continuity scenario is the Group-wide use of cloud-based technology and remote access tools such as laptops. Alpha's resilience to perform remotely is tested regularly with employees conducting assignments in (for example) client offices that are separate from the Alpha office environments.

In the context of business continuity, remote access can be deployed quickly to provide the ability to use information and communications technology that will allow key business processes or functions to be sustained from remote locations, for a short or extended period of time.

4.3. Business impact analysis

The heads of business operations areas and heads of country are responsible for conducting and documenting business impact analyses that involve determining all the critical processes, people, systems and technology that are essential to running their location or area. This should also include the impact should any of the business activities within their scope be disrupted as well as contingency planning to minimise risk to business continuity. The plan and analysis will be stored centrally.

Impact analysis should be reviewed and updated accordingly following any changes to processes, senior hires or implementation of new systems / technology.

A recovery point objective (RPO) must be determined and maintained for each system and technology identified as critical to the business and included in the impact analysis. The RPO is the period of time that each system / technology could be accepted after an outage before recovery is required and will be used when deciding whether to implement a recovery strategy after an outage occurs.

5. Disaster Recovery

5.1. Off-site facilities

Currently, no Alpha site has a temporary office location. In the event of a disruptive event causing offices to become inaccessible, impacted employees will work from home or (other location that is deemed safe) until instructed otherwise.

5.2. Communication strategy

5.2.1 Systems and Technology

The IT & Infrastructure team is responsible for informing Alpha employees of outages, performance issues and any other incidents that will impact business continuity. In exceptional cases, business support teams for key systems / technology may provide these communications.

Communication should detail the problem encountered, expected recovery timeframe, potential impact and any contingency plans being implemented.

5.2.2 Other Disruptive Events

The GCC is responsible for organising and delegating to an appropriate and effective communication team for the dissemination of information in the instance of a disruptive event. The team will comprise at least one director from the affected site(s) and at least one member of the GCC.

The communications team will then be responsible for disseminating information down to the employees. If a director is unavailable, it will be the BCP Owner’s responsibility to find a replacement or fulfil the role themselves.

If regular communication options (Slack, Email) are unavailable, the BCP Owner can also assign a director from the site(s) to provide information directly to impacted employees.

Communication to Omega contractors will be the responsibility of the Alpha engagement owners with whom the contractors are working at that time, as defined in Salesforce.

As well as communicating instructions in the instance of a disruptive event, the communication team should also ensure Alpha staff within their scope of responsibility are kept up to date with continuity plans and further developments.

5.3. Testing

The business continuity plan will be tested at least on an annual basis. The test will involve ensuring offsite / home-based facilitates like internet, telephony and systems meet and can sustain key business requirements. It will also involve testing that any business operations processes, such as finance team activities, can be conducted with minimal disruption. Any issues must be captured and raised with the appropriate director immediately so that remedial action can be arranged.

6. Appendices

Appendix 1 – Disruptive Events

- Fire
- Flood
- Explosion
- Terrorism
- Workplace violence
- Pandemic disease
- Utility outage
- Supplier failure
- Cyber attack

Business Continuity Policy

Issued: June 2016

Amended: May 2022

Privacy Policy

Introduction

This privacy statement explains how Alpha Financial Markets Consulting PLC and other Alpha group entities (as set out at Section 6) (together, "Alpha" "we" "our" "us") collects, uses, discloses and retains personal information, including personal information collected through the Alpha website and in connection with the management of Alpha's clients, prospective employees and contractors. Alpha is committed to respecting and protecting your privacy and complies with all applicable data protection and privacy laws.

This privacy statement is divided into four Sections:

1. Alpha Website Privacy Statement
2. Alpha CRM Privacy Statement
3. Alpha Recruitment Privacy Statement
4. Alpha Contractor Privacy Statement

Please carefully review all Sections that apply to you.

If you provide us with the personal information of other persons (such as family members or work colleagues), please make sure the respective persons are aware of this privacy statement and only provide us with their data if you are allowed to do so and such information is correct.

Alpha reserves the right to modify or update this privacy statement at any time without notice and any changes will be posted on this page.

1. Alpha Website Privacy Statement

Application

This Section 1 explains how Alpha collects, uses, discloses and retains personal information when you access and use the Alpha website.

Collection of personal information and purposes of collection

Some areas of our website may require you to give us personal information, which is information that enables us to identify you, including but not limited to your name, email or other address. Should you provide Alpha with your contact information through our website (such as name, company, address, and email address) this information will only be used to contact you for the purpose for which you have expressed an interest, such as the services, career opportunities, surveys and seminars of Alpha. Alpha may also collect domain information from your visit to customise and improve your experience on our website.

We will process your personal information as necessary for the purpose of our legitimate interests (including to respond to your queries and promote our business) and on the basis of your consent to the extent required by applicable data protection and privacy laws (for example, where we use cookies on our website). For more information, please refer to the "Cookies" section of this Section 1.

The amount and type of personal information collected, used, and disclosed shall be limited to what is necessary to achieve the purposes outlined in this Section 1.

Data security

Alpha is committed to protecting your personal information and ensuring that we securely store any personal information we collect in accordance with applicable data protection and privacy laws. We may hold your personal information in hard copy (paper) or electronic form.

Whilst Alpha takes all reasonable precautions to protect personal information from loss, misuse, alteration or destruction and complies with all applicable data protection and privacy laws, data transmission over the internet may not be adequately secured by the sender. As a result, Alpha cannot ensure the secure receipt of any information that is sent to Alpha by this medium and any such information is sent at your own risk.

Data recipients

Your personal information may be shared across the Alpha group throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia) and with certain third parties. Where third parties are given access to your personal information, Alpha will take the required contractual, technical and organisational measures to ensure that your personal information is processed only to the extent necessary and in accordance with applicable data protection and privacy laws.

In particular, the following categories of recipients may process your personal information:

- service providers that provide services on our behalf, including IT service providers;
- legal and other professional advisors and auditors; and
- regulators and law enforcement agencies.

Privacy Policy

Third country transfers

Alpha may process your personal information outside of the country in which you are resident or the country in which your personal information was collected, where data protection and privacy laws may not offer the same level of protection available in your home country or the country where your personal information was collected. Your personal information may be shared overseas with certain third parties located throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia). For example, the hosting locations of our IT infrastructure may be outside of the jurisdiction where we collected your personal information. Alpha maintains a list of the locations of its sub-processors which is available on request. Where your personal information is transferred overseas by us or on our behalf, we use appropriate safeguards to protect your personal information to a standard essentially equivalent to the law applicable to the country in which you are resident. These safeguards include implementing applicable standard contractual clauses for transfers of personal information between our group companies, which require group companies to protect personal information they transfer from the jurisdiction in which it was collected in accordance with applicable data protection and privacy laws and take reasonable steps to ensure that the overseas recipient does not breach applicable data protection and privacy laws in relation to your personal information. You may obtain information, and a copy of the relevant safeguard relied on for the transfer of your personal data by contacting us via the details set out in the "Contact us" Section.

Retention period

Alpha is committed to protecting your personal information and ensuring that we securely store any personal information we collect in accordance with applicable data protection and privacy laws.

Alpha will only hold your personal information for as long as required to undertake the purposes of our processing, to comply with our legal obligations, to enforce or protect our legal rights, or a longer period if required or permitted by applicable law.

Business Relationships

Our website may sometimes contain links to other websites. Please review the policies of these websites individually – Alpha is not responsible for the privacy practices or the content of such websites.

Cookies

Cookies store small amounts of data on your computer about your visit to the Alpha website. You can give consent to cookies, or withdraw any consent you have previously given, through our cookies tool or your browser settings.

Cookies can be categorised in accordance with how long they are saved on your device: "session cookies" are short-term cookies that are only saved on the device's memory for the duration of a user's visit to the website, whereas "persistent cookies" remain saved in the device's memory for a set period of time, even after the browser session has ended. The expiry period for each cookie is set out below.

What cookies do we use?

Strictly necessary cookies – enable core functionality such as security, network management, and accessibility. You can disable these by changing your browser settings, but this may affect how the website functions. You cannot disable these using our cookies tool. We use the following strictly necessary cookies:

Name	Source	Purpose	Expiry
PHPSESSID	PHP	This is a general-purpose identifier used to maintain user session variables; for example, maintaining a logged in status for a user between pages.	Session
ASP.NET_SessionId	otp.tools.investis .com	Used to maintain an anonymised user session by the server.	Session
AWSALBCORS and AWSALBTGCORS	otp.tools.investis .com	Used for load balancing, specifically for continued stickiness support.	7 days

Performance cookies – these cookies are set to understand how users interact with the website. We use the following performance cookies:

Name	Source	Purpose	Expiry
_ga	Google Analytics	This cookie is used to distinguish unique users by assigning a randomly generated number as a client identifier. It is included in each page request in a site and is used to calculate visitor, session and campaign data for analytics reports.	2 years
_gid	Google Analytics	Used to distinguish users of the Alpha website.	1 day
_cf_bm	CloudFlare	This cookie is used to distinguish between humans and bots. This is used to make valid reports on the use of the Alpha website.	30 minutes

Targeting cookies – these cookies are set to tailor marketing to you and your interests. We use the following targeting cookies:

Name	Source	Purpose	Expiry
YSC	.youtube.com	This cookie is set to track views of embedded videos.	Session
VISITOR_INFO1_LIVE	.youtube.com	This cookie is set to keep track of user preferences for YouTube videos embedded in sites; it can also determine whether the Alpha website visitor is using the new or old version of the YouTube interface.	6 months

Refusing or restricting cookies

You may refuse to accept, or withdraw your previous consent to, cookies in two ways:

- our cookies tool, which you can access at the bottom of our website. Our cookies tool will record when you have consented to non-essential cookies. Essential or strictly necessary cookies cannot be disabled using the tool because they are necessary to make the website function. You may change your mind about the cookies you have selected through our cookies tool by updating your choices in our tool at any time. Please be aware that our cookies tool cannot be used to block cookies on third party websites linked to our website. In order to remove these cookies, you will need to visit the relevant third party site and follow the instructions in their cookie notices. Alternatively, turn off these cookies using your browser settings; or
- you may refuse the use of cookies by selecting the appropriate settings in your browser.

Individual data rights

Depending on which laws apply to your personal information, you may have certain statutory rights in relation to your personal information. Subject to any exemptions provided by applicable law, if your personal information is processed by Alpha in respect of your use of our website, you may have the following rights:

- to receive confirmation from Alpha as to whether we process your personal information, and where we do, access to that personal information and certain other information;
- to request the rectification of any inaccurate personal information that we hold about you;
- to request the erasure of your personal data in certain circumstances;
- to request the restriction of our processing of your personal data in certain circumstances, for example in certain scenarios where we are unable to comply with a request to erase your personal data;
- to receive a copy of the personal information that you have provided to Alpha in a structured, machine-readable and commonly-used format and/or, where possible, to request we transmit that personal data to another organisation;
- to object to certain processing of your personal data and to automated decision making; and
- where our processing is based on your consent, subject to applicable law, you have the right to withdraw consent at any time by contacting us.

Privacy Policy

Where you are given the option to share your personal information with us, you can always choose not to do so. If you object to the processing of your personal information, to the extent permitted by applicable data protection and privacy law, we will respect that choice. This could mean that we are unable to perform the actions necessary to achieve the purposes of processing described in this Section 1.

Right to lodge a complaint

If you have any concerns or complaints regarding this privacy statement or our handling of your personal information, you may have recourse to additional remedies under applicable data protection and privacy laws.

You may make a complaint about our privacy practices using the contact details set out below. We will investigate and respond to a complaint within any relevant time periods stipulated by applicable data protection and privacy laws.

You may also have the right to contact or lodge a complaint with your local data protection authority (as set out at Section 5).

Contact Us

If you have any questions or comments about our privacy statement or practices, this Section 1 or Alpha's personal information handling practices, please contact us at:

Head of Legal

legal@alphafmc.com

60 Gresham Street, London EC2V 7BB

+44 (0) 207 796 9300

info@alphafmc.com

2. Alpha CRM Privacy Statement

Application

This Section 2 applies to you if you are an Alpha client. Please note that "client" may refer to any of the following: client organization, TPA or Vendor, or a third party such as a recruitment agency or industry body.

2.1. Categories of personal information

When we refer to "personal data" or "personal information" we mean any information relating to an identified or identifiable individual. This could include information that could identify an individual, directly or indirectly, in particular, by reference to an identifier such as a name, ID number, location data or online identifier (however, in some jurisdictions, such as Canada, this does not include information that is publicly available in a telephone directory or that is business contact information that enables an individual to be contacted at a place of business). It also includes factors specific to an individual's characteristics.

Alpha collects limited personal information on its clients; and this primarily encompasses the following types of information (to the extent such information constitutes personal information under applicable data protection and privacy laws):

- contact and organisation related material such as an individual's work email and business role; and
- business communications, such as email exchanges or in-person meetings.

2.2. Sources of personal information

We collect your personal information in a variety of ways during the course of your dealings with us. For example, when you engage with us in respect of a project we are undertaking for your organisation. We also gather information about you when you provide it directly to us, for example when you correspond with your contacts within Alpha.

We may also receive information about you from other sources, such as directly from your organisation or via online resources including LinkedIn and other publicly available sources. We combine information about you from various sources, including the information that you have provided to us directly.

2.3. Purposes of processing

Alpha collects, uses and otherwise processes client personal information for the following purposes:

- to manage past, current and future business engagements;
- to send information such as engagement related proposals and materials, industry relevant information (such as regulatory digest newsletters), and event invitations;
- to send direct marketing communications; and
- to comply with our legal and regulatory obligations.

2.4. Lawful basis for processing

Alpha only collects, uses, and otherwise processes personal information for the purposes outlined above and in accordance with applicable data protection and privacy laws.

Privacy Policy

We process personal information on the following bases:

- for legitimate business purposes, including ensuring that Alpha can: (i) maintain its relationships with existing clients, (ii) manage past, current and future client engagements and (iii) promote its services and products;
- for the performance of a contract that we have entered into with our client; and
- consent (including, to the extent required by applicable data protection law, for the purposes of sending direct marketing to individuals in a personal capacity by email, SMS or other electronic message).

2.5. Data recipients

Your personal information may be shared across the Alpha group throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia) and with certain third parties such as:

- service providers that provide services on our behalf, including IT service providers;
- legal and other professional advisors and auditors; and
- regulators and law enforcement agencies.

Where third parties are given access to your personal information, Alpha will take the required contractual, technical and organisational measures to ensure that your personal information is only processed to the extent necessary and in accordance with applicable data protection and privacy laws.

2.6. Third country transfers

Alpha may process your personal information outside of the country in which you are resident or the country in which your personal information was collected, where data protection and privacy laws may not offer the same level of protection available in your home country or the country where your personal information was collected. Your personal information may be shared overseas with certain third parties located throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia). For example, the hosting locations of our IT infrastructure may be outside of the jurisdiction where we collected your personal information. Alpha maintains a list of the locations of its sub-processors which is available on request. Where your personal information is transferred overseas by us or on our behalf, we use appropriate safeguards to protect your personal information to a standard essentially equivalent to the law applicable to the country in which you are resident. These safeguards include implementing applicable standard contractual clauses for transfers of personal information between our group companies, which require group companies to protect personal information they transfer from the jurisdiction in which it was collected in accordance with applicable data protection and privacy laws and take reasonable steps to ensure that the overseas recipient does not breach applicable data protection and privacy laws in relation to your personal information.

You may obtain information and a copy of the relevant safeguard relied on for the transfer of your personal data by contacting us via the details set out in the “Contact us” Section.

2.7. Retention period

Alpha is committed to protecting your personal information and ensuring that we securely store any personal information we collect in accordance with applicable data protection and privacy laws. We may hold your personal information in hard copy (paper) or electronic form.

Alpha will only hold your personal information for as long as required to undertake the purposes of our processing and to comply with Alpha’s legal obligations or enforce or protect Alpha’s legal rights, or a longer period required or permitted by applicable law.

We hold personal information about our clients for the following periods:

- data relating to prospective clients will be retained for up to five years, after which the record will be deleted if there is no recorded contact between Alpha and the prospective client;
- data relating to clients will be retained for the duration of the client relationship plus a further period to comply with certain obligations, legal requirements and best practices.

We will also retain your personal information for as long as necessary in connection with any legal action or any investigations involving Alpha.

We take steps to destroy or anonymise data that we no longer require or as required by applicable data protection and privacy law.

Privacy Policy

2.8. Individual data rights

Depending on which laws apply to your personal information, you may have certain statutory rights in relation to your personal information. Subject to any exemptions provided by applicable law, if your personal information is processed by Alpha in respect of our client relationship activities, you may have the following rights:

- to receive confirmation from Alpha as to whether we process your personal information, and where we do, access to that personal information and certain other information;
- to request the rectification of any inaccurate personal information that we hold about you;
- to request the erasure of your personal data in certain circumstances;
- to request the restriction of our processing of your personal data in certain circumstances, for example in certain scenarios where we are unable to comply with a request to erase your personal data;
- to receive a copy of the personal information that you have provided to Alpha in a structured, machine-readable and commonly-used format and/or, where possible, to request we transmit that personal data to another organisation;
- to object to certain processing of your personal data and to automated decision making; and
- where our processing is based on your consent, subject to applicable law, you have the right to withdraw consent at any time by contacting us.

Where you are given the option to share your personal information with us, you can always choose not to do so. If you object to the processing of your personal information, to the extent permitted by applicable data protection and privacy laws, we will respect that choice. This could mean that we are unable to perform the actions necessary to achieve the purposes of processing described in Section 2.3 above.

2.9 Right to lodge a complaint

If you have any concerns or complaints regarding this privacy statement or our handling of your personal data, you may have recourse to additional remedies under applicable data protection and privacy laws.

You may make a complaint about our privacy practices to us at the contact details set out below. We will investigate and respond to a complaint within any relevant time periods stipulated by applicable data protection and privacy laws.

You also have the right to contact or lodge a complaint with your local data protection authority (as set out at Section 5).

2.10. Contact us

Please feel free to contact us if you have any questions about this Section 2 or any of our practices in relation to your personal information. Clients should direct requests to their primary contact at Alpha in the first instance, whether this is to seek further information or to exercise any of your statutory rights.

You can also contact us at:

Head of Legal

legal@alphafmc.com

60 Gresham Street, London EC2V 7BB

+44 (0) 207 796 9300

info@alphafmc.com

3. Alpha Recruitment Privacy Statement

Application

This Section 3 applies to you if you apply for a position with Alpha.

Personal Information

Alpha is committed to the fair treatment of individuals' personal information and complies with all applicable data protection and privacy laws and regulations. Alpha is also committed to ensuring the security of individuals' data and has taken appropriate technical and organisational measures to this end. This document provides the required information on the treatment of any personal information that you submit to Alpha or that Alpha may request from you.

3.1. The personal information we collect, hold and otherwise process about you

When we refer to "personal information", we mean any information that allows an individual to be identified, either directly or indirectly, in particular by reference to an identifier such as a name or identification number or other characteristic that may reveal identity. In respect of our job candidates' personal information, we typically collect, hold and otherwise process personal information including:

- contact details such as your name, address, email address and telephone number;
- your date of birth;

Privacy Policy

- recruitment information such as copies of documents proving your right to work, references, CV information, cover letter or correspondence with us as part of the application and recruitment process (such as information about your qualifications, experience, knowledge, skills and abilities);
- financial information such as your current salary, and your bank account details for the purposes of reimbursing expenses;
- other people's opinions about you, including references;
- travel information such as your name, address, car registration number, personal details required for any public transport tickets;
- CCTV footage, including photo stills and other information obtained through electronic means such as entry and exit data if you attend an interview at our premises;
- background checks, including information raised in criminal record checks and government screening checks;
- information relating to your health and medical conditions as is necessary to ensure your fitness for work and compliance with our health and safety obligations during your application process; and
- in some jurisdictions, we may collect diversity related data, including information about your racial or ethnic origin, sexual orientation and marital status which is tracked on an aggregated basis to ensure we are attracting diverse candidates.

3.2. Sources of processing

We collect your personal information during the recruitment process for which you have put yourself forward. For example, your CV and cover letter, your communications with Alpha HR staff and, as appropriate, your performance in assessments.

We may also receive information about you from other sources, such as background checking and online resources including LinkedIn and other publicly available sources. We combine information about you from various sources, including the information that you have provided to us directly.

3.3. Purpose of processing

Candidate personal information is collected, held, used and otherwise processed for the following purposes:

- assessing your suitability for employment;
- checking you are legally entitled to work in the jurisdiction in which the role you have applied for is based;
- ascertaining your fitness for work;
- monitoring equal employment opportunities;
- establishing, exercising or defending legal rights and disputes; and
- ensuring compliance with our internal policies and procedures.

3.4. Lawful basis for processing

Alpha collects, uses, processes and discloses personal information only for the purposes outlined in this policy and in accordance with applicable data protection and privacy laws. We limit our collection to what is reasonably required to fulfil the purposes for which it was collected. We process personal information on the following bases:

- in accordance with your explicit consent;
- for our legitimate business purposes of our employee recruitment activities; and
- to comply with certain legal and regulatory obligations of Alpha.

3.5. Data recipients

Your personal information may be shared with Alpha's affiliates throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia), and with certain third parties such as:

- service providers that provide services on our behalf, including IT service providers;
- legal and other professional advisors and auditors; and
- regulators and law enforcement agencies.

Where third parties are given access to your personal information, Alpha will take the required contractual, technical and organisational measures to ensure that your personal information is only processed to the extent necessary. Third parties will only process your personal information in accordance with applicable law.

3.6. Third country transfers

Alpha may process your personal information outside of the country in which you are resident or the country in which your personal information was collected, where data protection and privacy laws may not offer the same level of protection available in your home country or the country where your personal information was collected. Your personal information may be shared overseas with certain third parties located throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia). For example, the hosting locations of our IT infrastructure may be outside of the jurisdiction where we collected your personal information. Alpha maintains a list of the locations of its sub-processors which is available on request. Where your personal information is transferred overseas by us or on our behalf, we use appropriate safeguards to protect your personal information to a standard essentially equivalent to the law applicable to the country in which you are resident.

Privacy Policy

These safeguards include implementing applicable standard contractual clauses for transfers of personal information between our group companies, which require group companies to protect personal information they transfer from the jurisdiction in which it was collected in accordance with applicable data protection and privacy laws and take reasonable steps to ensure that the overseas recipient does not breach applicable data protection and privacy laws in relation to your personal information. You may obtain information and a copy of the relevant safeguard relied on for the transfer of your personal data by contacting us via the details set out in the “Contact us” Section.

3.7. Retention period

- Alpha is committed to protecting your personal information and ensuring that we securely store any personal information we collect in accordance with applicable data protection and privacy laws. We may hold your personal information in hard copy (paper) or electronic form.

Your personal information will be retained by Alpha for 3 years from the close of the recruitment process so that we may contact you in the future if there are further opportunities, unless you have informed us that you are no longer interested in a role with Alpha. Alpha may also delete certain records from your recruitment process within this timeframe if we deem that they are no longer required. Records will always be retained, destroyed and/or anonymised in line with relevant statutory retention periods.

3.8. Individual data rights

Depending on which laws apply to your personal information, you may have certain statutory rights in relation to your personal information. Subject to any exemptions provided by applicable law, if your personal information is processed by Alpha, you may have the following rights:

- to receive confirmation from Alpha as to whether we process your personal information, and where we do, access to that personal information and certain other information;
- to request the rectification of any inaccurate personal information that we hold about you;
- to request the erasure of your personal data in certain circumstances;
- to request the restriction of our processing of your personal data in certain circumstances, for example in certain scenarios where we are unable to comply with a request to erase your personal data;
- to receive a copy of the personal information that you have provided to Alpha in a structured, machine-readable and commonly-used format and/or, where possible, to request we transmit that personal data to another organisation;
- to object to certain processing of your personal data and to automated decision making; and
- where our processing is based on your consent, subject to applicable law, you have the right to withdraw consent at any time by contacting us.

Where you are given the option to share your personal information with us, you can always choose not to do so. If you object to the processing of your personal information, to the extent permitted by applicable data protection and privacy laws, we will respect that choice. This could mean that we are unable to perform the actions necessary to achieve the purposes of processing described in Section 3.3.

3.9. Right to lodge a complaint

If you have any concerns or complaints regarding this privacy statement or our handling of your personal data, you may have recourse to additional remedies under applicable data protection and privacy laws.

You may make a complaint about our privacy practices using contact details set out below. We will investigate and respond to a complaint within any relevant time periods stipulated by applicable data protection and privacy laws.

You also have the right to contact or lodge a complaint with your local data protection authority (as set out at Section 5).

3.10. Contact Us

If you have any questions or comments about this Section 3 or Alpha’s personal information handling practices, please contact us via email at:

Head of Legal

legal@alphafmc.com

60 Gresham Street, London EC2V 7BB

+44 (0) 207 796 9300

info@alphafmc.com

Alternatively, if you have any questions about anything contained within this Section 3 please don’t hesitate to reach out to your contact point at Alpha.

Privacy Policy

4. Alpha Contractor Privacy Statement

Application

This Section 4 applies to you if you are a contractor engaged by Alpha to perform services.

Personal Information

Alpha is committed to the fair treatment of individuals' personal information and complies with all applicable data protection and privacy laws and regulations. Alpha is also committed to ensuring the security of individuals' data and has taken appropriate technical and organisational measures to this end.

This Section 4 explains how we collect, use and otherwise process your personal information. We limit our collection of personal information to what is reasonably required to fulfil the purposes for which it was collected.

You are advised to review this Section 4 periodically as it may change from time to time. You will also receive training on data protection.

.1. The personal information we collect, hold and otherwise process about you

When we refer to "personal information" or "personal data" we mean any information relating to an identified or identifiable individual. This could include information that could identify an individual, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data or online identifier. It also includes factors specific to an individual's characteristics, (however, in some jurisdictions, such as Canada, personal information would not include information that is publicly available in a telephone directory or that is business contact information that enables an individual to be contacted at a place of business).

In respect of our contractors, we typically collect, hold and otherwise process personal information including:

- your personal contact information, including name, title, addresses, telephone numbers, and personal email addresses;
- your personal details, including name, title, surname, birth date, government issued national identification or passport number, gender, civil status, beneficiaries and dependents, emergency contact information and photograph;
- engagement information, including copies of your right to work documentation, background checks, references and other information included in your CV, cover letter or correspondence with us as part of the engagement process (such as information about your qualifications, experience, knowledge, skills and abilities);
- to the extent necessary, disciplinary and grievance records including details contained in or relating to any disciplinary or grievance investigations or proceedings;
- information about your engagement terms;
- bank account details, payroll records and tax status information;
- records containing information about incidents that involve or relate to you;
- information about your usage on our information and communications systems or other electronic systems;
- references or feedback on your performance by colleagues or customers;
- information about business travel and expenses, including name, address, vehicle registration number (if applicable for company or private car), personal details required for any travel, hotel, insurance, personal or corporate banking details or personal and corporate credit card details;
- position/role details, work contact details, work history, engagement and termination reasons, and date and length of service;
- absence and leave records, as they may be agreed to apply to you;
- CCTV footage and other information obtained through electronic means, such as entry and exit data, if you perform services on Alpha premises; and
- office data, including workplace telephone numbers, work address and room location, office status and work email address (to the extent such information constitutes personal information under applicable law).

4.2. Sources of personal information

We collect your personal information during the course of your engagement with us. For example, material submitted during the onboarding process, or records generated when you engage with our internal departments. We gather information about you when you provide it to us, for example your CV and details to arrange payment for your services.

We may also receive information about you from other sources, such as online resources including LinkedIn and other publicly available sources. We combine information about you from various sources, including the information that you have provided to us directly.

Privacy Policy

4.3. Purpose of processing

Contractor information is collected, held, used and otherwise processed for the following purposes:

Background checks and onboarding

such as assessing your suitability for the engagement, checking you are legally entitled to work in the jurisdiction in which your engagement is based, confirming your fitness for work, establishing a contractual relationship and determining the terms of your engagement.

Personnel administration

such as invoice administration, general administration of your service contract, facilitating communications, to deploy potential contractors on client projects, supporting any business or administrative function required (e.g. business visas), making business travel arrangements, and administering and managing our business operations;

Compliance with legal and regulatory obligations

including complying with health and safety obligations, complying with applicable laws and regulations;

General business purposes

including ensuring business continuity, strategic planning and project management, budgeting and financial management and reporting;

Post-engagement relations

including to contact contractors about future opportunities;

Managing Alpha's network and IT systems

such as operating and managing the information and communications systems to allow you to use them, to confirm you are using appropriately our information and communications systems and other electronic systems such as the internet, and ensuring network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution; and

To establish, exercise, or defend legal rights and disputes

Alpha also may require you to submit and periodically update a CV so that we can provide clients with information relevant to our project engagements. This experience, as well as your LinkedIn profile, may also be used by 'Stitched', a third party provider we are engaging to create experience profiles. While you work as a contractor for Alpha, you may be asked to participate.

We collect, use, process and disclose personal information only for the purposes outlined in this privacy statement and in accordance with applicable data protection and privacy laws. We do not collect, use, disclose or otherwise process, personal information for any purpose or in any way other than as described in this document (or, to the extent permitted under applicable data protection and privacy laws, any purpose directly related to, or compatible with, such purpose), unless we are required or permitted by applicable data protection and privacy laws to do so, you are so informed at the time of collection, or we have obtained your consent, directly or indirectly, to use or disclose your personal information for another purpose or in another manner.

4.4. Lawful basis for processing

Alpha collects, uses, discloses and otherwise processes personal information in accordance with applicable data protection and privacy laws and regulations. We process personal information on the following bases:

- for the legitimate interests of Alpha, including administration, conducting onboarding checks, and to enable the functioning of our business;
- for the performance of our contract with you; and
- to comply with certain legal and regulatory obligations of Alpha.

Please note that any failure on the part of any contractor to provide information that Alpha requires in order to meet its contractual obligations may result in Alpha being unable to comply with those requirements. This may result in a delay in your start date working for us, delay in the payment of any funds owed to you, or may ultimately prevent us from engaging your services.

4.5. Data recipients

Your personal information will be shared with other entities within the Alpha group (including Alpha entities in Europe, the United Kingdom, the United States, Canada, Singapore and Australia), your Engagement Lead and appropriate levels of your management chain, and personnel and other departments throughout Alpha.

In addition, your personal information will be shared with third parties, including companies that provide products and services to us (such as computer backup services, archival storage services, advisory services, payroll services, pension and benefits administration, human resource management services, recruitment services, termination services, IT systems suppliers and support and/or other third party services related to services rendered by us) and with Alpha's clients.

Privacy Policy

From time to time, we may also need to make your personal information available to other third parties, such as legal and regulatory authorities, accountants, auditors, lawyers and other outside professional advisors.

All our third-party service providers and entities in our group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal information for their own purposes. We only permit them to process your personal information for specified purposes.

4.6. Third country transfers

Alpha may process your personal information outside of country in which you are resident or the country in which your personal information was collected, where data protection and privacy laws may not offer the same level of protection available in your home country or the country where your personal information was collected. Your personal information may be shared overseas with certain third parties located throughout the world (including in Europe, the United Kingdom, the United States, Canada, Singapore and Australia). For example, the hosting locations of our IT infrastructure may be outside of the jurisdiction where we collected your personal information. Alpha maintains a list of the locations of its sub-processors which is available on request. Where your personal information is transferred overseas by us or on our behalf, we use appropriate safeguards to protect your personal information to a standard essentially equivalent to the law applicable to the country in which you are resident. These safeguards include implementing applicable standard contractual clauses for transfers of personal information between our group companies, which require group companies to protect personal information they transfer from the jurisdiction in which it was collected in accordance with applicable data protection and privacy laws and take reasonable steps to ensure that the overseas recipient does not breach applicable data protection laws in relation to your personal information. You may obtain information and a copy of the relevant safeguard relied on for the transfer of your personal data by contacting us via the details set out in the "Contact us" Section.

4.7. Retention period

Alpha is committed to protecting your personal information and ensuring that we securely store any personal information we collect in accordance with applicable data protection and privacy laws. We may hold your personal information in hard copy (paper) or electronic form.

Alpha will only hold your personal information for as long as required to undertake the purposes of our processing, plus a prescribed period of time as required or permitted by applicable laws in your jurisdiction.

We hold personal information about contractors for the following periods:

- contractor contact and CV data will be held by Alpha for up to 3 years following termination or expiration of your engagement by us, at which point we contact individuals to ask whether they would still be interested in offering contractor services to Alpha and update our records accordingly.
- Finance and certain other records will be retained for as long as necessary for Alpha's accounting purposes and to ensure that contractors are correctly remunerated for their time and expenses, plus a period of 7 years in case any legal action arises relevant to this information.

We will also retain your personal information for as long as it is required in connection with legal action or any investigations involving Alpha.

We take steps to destroy or anonymise data that we no longer require or as required by applicable data protection and privacy law.

4.8. Individual data rights

Depending on which laws apply to your personal information, you may have certain statutory rights in relation to your personal information. Subject to any exemptions provided by applicable law, if your personal information is processed by Alpha, you may have the following rights:

- to receive confirmation from Alpha as to whether we process your personal information, and where we do, access to that personal information and certain other information;
- to request the rectification of any inaccurate personal information that we hold about you;
- to request the erasure of your personal data in certain circumstances;
- to request the restriction of our processing of your personal data in certain circumstances, for example in certain scenarios where we are unable to comply with a request to erase your personal data;
- to receive a copy of the personal information that you have provided to Alpha in a structured, machine-readable and commonly-used format and/or, where possible, to request we transmit that personal data to another organisation;
- to object to certain processing of your personal data and to automated decision making; and
- where our processing is based on your consent, subject to applicable law, you have the right to withdraw consent at any time by contacting us.

Privacy Policy

4.9. Right to lodge a complaint

If you have any concerns or complaints regarding this privacy statement or our handling of your personal data, you may have recourse to additional remedies under applicable data protection and privacy laws.

You may make a complaint about our privacy practices to us at the contact details set out below. We will investigate and respond to a complaint within any relevant time periods stipulated by applicable data protection and privacy laws.

You also have the right to contact or lodge a complaint with your local data protection authority (as set out at Section 5).

4.10. Contact Us

If you have any questions or comments about our privacy statement or practices, please contact us at:

Head of Legal

legal@alphafmc.com

60 Gresham Street, London EC2V 7BB

+44 (0) 207 796 9300

info@alphafmc.com

5. Data protection authorities

UK

– Information Commissioner's Office (ICO). Information on raising a complaint is available on the ICO's website (https://ico.org.uk/concerns/)

EU

– A list of EU data protection authorities by jurisdiction is available at http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

Canada

– Federal Privacy Commissioner or your provincial Privacy Commissioner, as applicable

Australia

– The Office of the Australian Information Commissioner, which can be contacted by telephone on 1300 363 992 or by using the contact details on the website www.oaic.gov.au

Switzerland

– Federal Data Protection and Information Commissioner (http://www.edoeb.admin.ch).

Issued: October 2022

Privacy Policy

6. Relevant Alpha entities

The list below details the Alpha entities which may act as a controller for your data in conjunction with Alpha Financial Markets Consulting PLC.

COMPANY NAME	COMPANY NUMBER	REGISTERED ADDRESS
AIVIQ Limited	(11480862)	60 Gresham Street, London, EC2V 7BB, UK
Alpha Financial Markets Consulting (Luxembourg) S.A.	(B137955)	19/21 route d'Arlon – bloc B, L-8009 Strassen, Luxembourg
Alpha Financial Markets Consulting Australia PTY Limited	(631221862)	383-385 George Street, Sydney NSW 2000
Alpha Financial Markets Consulting Group Limited	(07160664)	60 Gresham Street, London, EC2V 7BB, UK
Alpha Financial Markets Consulting Hong Kong Limited	(2549029)	22/F., Neich Tower, 128 Gloucester Road, Wanchai, Hong Kong
Alpha Financial Markets Consulting Netherlands BV	(61668451)	Strozzilaan 101, Amsterdam, 1083 HN, The Netherlands
Alpha Financial Markets Consulting S.A.S.	(523666063)	6 Square de l'Opera Louis Jouvet, 75009 Paris, France
Alpha Financial Markets Consulting Singapore Pte Ltd	(201629440W)	OUE 6A Shenton Way, Level 04-01, Singapore, 068815
Alpha Financial Markets Consulting Switzerland S.A.	(CHE-432.187.554)	Bleicherweg 10, 8002 Zürich, Switzerland
Alpha Financial Markets Consulting UK Limited	(04710715)	60 Gresham Street, London, EC2V 7BB, UK
Alpha Financial Markets Consulting, Inc.	(26-4822447)	575 Fifth Avenue, New York, NY 10017, USA
Alpha FM Consulting Canada Inc	(BC1275236)	Suite 1700, Park Place, 666 Burrard Street, Vancouver, BC V6C2X8, Canada
Alpha Financial Markets Consulting (Insurance) France SAS	(907780217)	6 Square de l'Opéra Louis Jouvet, 75009 Paris, France
Alpha FMC Bidco Limited	(9928343)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Group Holdings Limited	(08555831)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Group Limited	(08506571)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Group Nominees Limited	(08936452)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Midco 2 Limited	(9963816)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Midco Limited	(9928345)	60 Gresham Street, London, EC2V 7BB, UK
Alpha FMC Trustee Limited	(10773199)	60 Gresham Street, London, EC2V 7BB, UK
Alpha Technology Services Consulting Limited	(09244222)	60 Gresham Street, London, EC2V 7BB, UK
Alpha Technology Services Consulting S.A.S.	(881001267)	6 Square de l'Opera Louis Jouvet, 75009 Paris, France
Axxsys Danmark ApS	(40121757)	Flaesketorvet 68, DK-1711 Copenhagen, Denmark
Axxsys Financial Software Consulting Canada Ltd	(BC0956822)	1800-13401 108th Avenue, Surrey, British Columbia V3T 5T3
Axxsys UK	(04967647)	New Broad Street House, 35 New Broad Street, London, EC2M 1NH, UK
Axxsys USA, Inc	(5349312)	Incorp Services Inc One Commerce Center,1201 Orange Street #600,Wilmington, Delaware 19899
Lionpoint GmbH	(Cologne: # HRB 107306) (Munich: # HRB 265516)	c/o KUNZ Rechtsanwälte, Antoniterstraße 14-16, Köln, 5066
Lionpoint Group (UK) Limited	(09869494)	5 Upper St. Martin's Lane, London, WC2H 9EA
Lionpoint Group Pty Limited	(635 472 383)	Ground Floor, 123 Walker Street, North Sydney NSW 2060
Lionpoint Group SA	(CHE-305.144.702)	Rue d'Italie 11, 1204 Geneva, Switzerland
Lionpoint Group, LLC	(5522271)	8 The Green, Suite A, Dover, Delaware 19901, United States of America
Lionpoint Holdings, Inc.	(7186662)	251 Little Falls Drive, Wilmington, DE 19808-1674, United States Of America
Obsidian Alpha Data Solutions LLC Belgrade	(11480862).	Serbia
Obsidian Solutions Ltd	(09737564)	60 Gresham Street, London, EC2V 7BB, UK
Track Two GmbH	(HRB 108642)	Mergenthalerallee 73-75, 65760 Eschborn, Germany

Alpha GPT – Data Privacy Impact Assessment

Background

Alpha has built AlphaGPT to improve business efficiency, for example by generating template documents such as presentations, meeting agendas, reports, translating documents etc.

Data Privacy Impact Assessment

Alpha has considered and concluded that a full Data Privacy Impact Assessment (DPIA) is not required as the purpose of AlphaGPT is not to process personal data and there is limited risk to the rights and freedoms of individuals. For example:

- There are no systematic or extensive processing activities, where decisions have legal effects, or similarly significant effects, on individuals;
- There is no large-scale processing of special categories of data or personal data relation to criminal convictions or offences.

People involved in this assessment:

- Matthew Mace: Group Head of Legal and Corporate Affairs
- Eloise Lipkin: Group Head of Risk and Responsible Business
- Tim Pringuer: Information Security Lead
- Rhona Sweeting: Knowledge Manager

Reasons for reaching this conclusion

AlphaGPT is a language model and interface that allows users to enter prompts and receive outputs based on those commands.

Unlike ChatGPT, Alpha GPT is ringfenced, meaning that it has been designed to operate within a specific set of parameters and is optimised for Alpha's particular use case.

Alpha GPT does not access:

- Alpha's data and document storage systems such as Box, SharePoint, Workday, Salesforce, etc.
- External web resources (although this may change in the near future; this would not impact the security analysis as it is a one-way query).

With AlphaGPT, Alpha's internal data stays strictly within the organization. There's no risk of external data leakage, ensuring the highest standards of privacy and confidentiality.

Residual risk

There is a residual risk that an individual could introduce personal data (regarding themselves or third parties) by uploading it to AlphaGPT.

This risk is mitigated by the following:

- Training and instruction
    - AlphaGPT user guide advises users to be aware that sensitive content (both client-related and personal) should be uploaded with care.
    - Annual data handling training which addresses data privacy generally.
- Information is stored in raw text format
- Weekly report run which only Rhona Sweeting and Till Blesik can access.

Conclusion

In its current iteration is there is a low risk of the introduction to AlphaGPT of personal data, or the processing by AlphaGPT of personal data. AlphaGPT does not access Alpha corporate document or data storage systems and users are cautioned against introducing personal data.

The small residual risk is addressed through weekly monitoring.

Future developments in AlphaGPT will, however, be reviewed from a data privacy perspective.

Issued: February 2025