

# Standards of Business Conduct

28 June 2019



# Contents

Chief Executive's Message .....	3
Introduction .....	4
Whistleblowing .....	7
Conflicts of Interest .....	9
Bribery and Corruption .....	11
Entertainment and Gifts.....	13
Political Contributions.....	15
Charitable Contributions.....	16
Accurate Accounting and Record-Keeping .....	17
Protection of Corporate Assets.....	19
Confidentiality and Information Security .....	20
Competition and Anti-Trust Laws .....	22
Money Laundering and Anti-Terrorism .....	24
Sanctions .....	26

# Chief Executive's Message

We believe that conducting our business with honesty and integrity is critical to the continuing development of a business that is responsible, successful and sustainable in the long term.

Our Standards of Business Conduct underpins our commitment to high standards of corporate behaviour as applied to specific situations which may arise in our day-to-day business life.


The Standards require all employees and representatives to act with high standards of business integrity, to comply with all laws and regulations wherever we operate and to ensure that our business standards are never compromised for the sake of results.

They are intended to provide guidance and to support our employees in making appropriate judgments and decisions in the course of their work, whilst ensuring that all actions are lawful and in line with our high expectations.

We all have a personal responsibility to ensure that our conduct is at all times in accordance with the Standards of Business Conduct. There should be no gap between what we say and what we do. Critical to applying the Standards is our commitment to an open culture where people feel secure in seeking advice and raising concerns. If you are unsure of what to do in particular circumstances or have concerns about suspected wrongdoing at work, then you have an obligation to speak up. Our policy and procedures for whistleblowing policy have been developed to enable you to communicate these concerns in confidence and without fear of reprisal, provided that concerns are raised in good faith.

The Standards of Business Conduct will be reviewed over time to ensure that they continue to reflect corporate conduct and values in compliance with applicable laws and regulations. You need to be aware of these Standards of Business Conduct and of any other Standards adopted by the group company for which you work.

It is important that we continue to uphold our high standards of corporate behaviour and to act in ways that maintain and enhance the reputation of the British Marine Group and its employees. Together, by following the letter and the spirit of the Standards of Business Conduct, we can help to ensure that the British Marine Group continues to grow its operating business and deliver strong financial returns, and is a Group for which we are proud to work.



Alan Bekhor  
28 June 2019

# Introduction

These Standards of Business Conduct set out the rules and policies that all employees of the British Marine Group must follow.

These Standards apply to all directors, officers and permanent employees of Group companies, but also to secondees, trainees, those on work experience and other temporary staff. Throughout the policy these identified persons shall be referred to as 'employees' or 'our people'. If you are responsible for engaging and/or supervising individuals in such roles, you should ensure that they are familiar with the Standards and their obligations under them.

In order to promote the application of consistently high standards of corporate conduct throughout the Group, each operating company within the Group is expected to adopt either these Standards of Business Conduct or its own Standards which reflect them.

Where strict application of these Standards would conflict with local law, the latter will take precedence, with deviation from these Standards permitted within the Standards adopted locally by a Group company to the extent necessary to comply with local law. In order to promote the application of consistently high standards of corporate conduct each operating company within the Group is expected to adopt either these Standards of Business Conduct or its own Standards which reflect them.

It is a fundamental policy of the British Marine Group that all Group companies and all employees must:

- observe and comply with the laws and regulations applicable to them; and
- act with high standards of business integrity.

Your obligation to act with high standards of business integrity goes beyond strict legal compliance, which means:

- behaving responsibly;
- conducting business in a manner which is honest, sincere, and trustworthy;
- acting in accordance with accepted standards of behaviour; and
- always choosing what you truly believe to be the right course of action.

The following sections set out the Group policy and provide guidance on a number of specific areas relevant to the conduct of the Group's business.

These Standards are, however, by no means exhaustive. All employees should make sure that they are familiar with, and that they adhere to:

- all other applicable Group Policies, Standards and Common Platforms;
- the rules and policies of the Group company for which they work; and
- all laws and regulations applicable to them and their area of work.

Although these Standards cannot cover every situation which you might encounter in your work, they do provide a sound basis for identifying the principles which should always govern your conduct. It is essential in your conduct that you follow their spirit of the Standards as well as their content.

Where you encounter a situation where you are unsure as to the proper course of action, you should ask yourself the following questions:

- Am I comfortable with what I propose doing?
- Would I be comfortable explaining my conduct to the board of my company, my family or friends or the media?
- Who does my conduct affect and would it be considered fair by those affected?

If the issue cannot be resolved in this way, then you should discuss the situation with your colleagues and, if necessary, seek guidance from your department manager or supervisor, or from your local Legal Counsel.

All employees of Group companies are expected to know, understand and follow these Standards or, as appropriate, the Standards adopted by the Group company for which they work.

Contractors, agents and consultants engaged on behalf of any Group company are expected to apply standards of business conduct consistent with the Standards, and wherever possible they are expected to sign a contractual commitment stating this fact. Employees should report any breaches or inconsistent behaviour by any such third party.

Those who supervise others have additional responsibilities under the Standards. They must:

- make sure that those reporting to them know and understand the Standards;
- monitor the conduct of those they supervise to satisfy themselves that it meets the Standards;
- enforce the Standards consistently;
- show by your own behaviour what it means to act with integrity; and
- support employees who, in good faith, raise questions about business conduct or concerns of wrongdoing.

In addition, you should make sure that those reporting to you have sufficient support and resources to enable them to adhere to the Standards. You should always be willing to take the time to listen to and guide those who come to you with questions or concerns arising under the Standards.

No department manager or supervisor has the authority to order or approve any action that is contrary to the Standards, or to any applicable law or regulation, and the Standards must not under any circumstances be compromised for the sake of results.

Employees have a duty to report incidences of noncompliance with the Standards and any other incidences of wrongdoing at work.

If you are instructed by your department manager or supervisor to do something which involves, or appears to involve, an illegal activity or a breach of the Standards, you should immediately bring the matter to the attention of local senior management or your local Legal Counsel, or a 'Designated Officer' under the Whistleblowing Policy or your local whistleblowing procedure.

The Standards absolutely prohibit retaliation against employees who in good faith report information or raise questions about possible violations of the law or the Standards.

Disciplinary action will be taken for violations of law or the Standards, as appropriate, including termination of employment. Any failure to follow the Standards that involves a criminal act could result in prosecution after referral to the relevant authorities.

At the end of each year, the designated department managers within each Group company are required formally to confirm that the company or department for which he is responsible complies with the Standards. In respect of employees in our UK Head Office, they are required to formally confirm that they as individuals are compliant with the Standards.

General Managers and Heads of Function must make every reasonable effort to ensure that their declaration of compliance is accurate and truthful. They should implement their own sign-off process within their company or department which is sufficiently comprehensive to enable them to satisfy themselves in this regard (save to the extent that any matter is being actively and wrongfully concealed).

## Terminology

1) In this document:

- 'Group' and 'British Marine Group' mean British Marine plc and all of its subsidiaries; and
- 'Group Company' and 'British Marine Company' mean any company within the British Marine Group.

2) Depending on the context, 'Standards' can mean the Group Standards set out in this document and/or the Standards adopted locally by a Group company.

3) All references to 'employees' in this document include, where the context admits, directors, officers and permanent employees of Group companies and also temporary staff, including secondees, trainees and those on work experience.

4) For convenience this document refers to employees as 'he' but it applies equally to all employees, regardless of gender.

# Whistleblowing

Any employee who suspects wrongdoing at work is strongly encouraged to raise his concern in confidence through the internal whistleblowing procedure.

Anyone who raises a genuinely held concern in good faith concerning a matter which he reasonably believes to be true will not suffer any form of reprisal or retribution as a result. This will be the case even where the individual raising the concern is mistaken and there is no case to answer.

Harassment or victimisation, including informal pressure, of anyone raising a genuine concern will not be tolerated, and any such conduct will itself constitute a breach of the Standards of Business Conduct and will be treated as a serious disciplinary matter.

While no one who comes forward in good faith has anything to fear, false allegations raised maliciously will be treated as misconduct and dealt with in accordance with the Disciplinary Procedure.

An individual who is concerned about actual or suspected wrongdoing and who wishes to report the matter formally for investigation should raise it with his line manager. The line manager should immediately refer the matter to a Designated Officer for investigation but must otherwise keep all details confidential.

Where an individual feels unable to raise his concern with his line manager, for whatever reason, it should be raised directly with a Director.

Concerns raised in this way will be investigated fully and the identity of the person raising the concern will be kept confidential.

When the investigation has been completed, the person who raised the concern will be informed of the outcome by the Director.

Group operating companies should implement local whistleblowing procedures to supplement this policy and the Group procedures identified above.

Examples of suspected wrongdoing that should be raised in this way include:

- the commission of a criminal offence;
- a failure to comply with any legal obligation or any other unlawful act or omission;
- an act or omission which will, or is likely to, unlawfully endanger the health or safety of an individual or unlawfully damage the environment;
- a breach of human rights;
- accounting malpractice or falsification of documents;
- any other breach of the Standards of Business Conduct or any other applicable Group Policy, Standard or Common Platform;
- a miscarriage of justice; and
- concealment of any of the above.

This list is not exhaustive. A concern should be raised irrespective of whether the suspected wrongdoing has occurred, is occurring or is likely to occur.

This procedure is not intended for use where you are unhappy with your personal employment position, for example lack of promotion or a smaller than expected wage increase – the Group's Grievance Procedures are available in those cases.

The Group Designated Officers, with whom any Group employee may raise a concern, are:

- the Chief Executive Officer; or
- the Chief Financial Officer.

They can each be contacted by e-mail, by telephone (+44 (0)20 7487 9717), or by writing to them at British Marine plc, 11 Manchester Square, London W1U 3PW.

While concerns may be raised anonymously, you are strongly encouraged to report matters in confidence rather than anonymously. A full investigation of your concern may not be possible without your cooperation, and proper feedback cannot be provided to those who remain anonymous.

A Group company's whistleblowing procedure should identify locally (and, where appropriate, regionally) based Designated Officers and enable staff to raise concerns in a language with which they feel comfortable.



# Conflicts of Interest

A conflict of interest will arise in any situation where your position or responsibilities within the Group present an opportunity for you or any close relative to obtain a personal gain or benefit (apart from the normal rewards of employment), or where there is scope for you to prefer your personal interests, or those of any close relative, above your duties and responsibilities to the Group.

Employees must avoid situations where their personal interests might, or might appear to, be in conflict with the interests of the Group or any Group company.

The guiding principle is that an employee must disclose to higher management any actual or potential conflict of interest.

Any situation which gives rise, or might give rise to a conflict of interest should be disclosed as soon as it arises and, where required, written authority to proceed should be sought.

Actual and potential conflicts of interest must also be disclosed each year during the year end formal confirmation of compliance with the Standards.

A potential conflict of interest will arise where an employee is in a situation which could develop into an actual conflict of interest, for example if he were to change role within the Group.

All Group companies must maintain a 'conflicts log' which records the details of all actual or potential conflicts of interest disclosed by their employees and the action taken in respect of them.

Accordingly, managers should ensure that any actual or potential conflicts of interest disclosed to them are notified to the person responsible for maintaining the relevant conflicts log.

Employees may not exploit knowledge or information gained from employment within the Group or take advantage of a corporate opportunity in order to obtain a personal gain or benefit for themselves or for any close relative, without first disclosing their intention to do so and obtaining written approval.

Employees may not work for or on behalf of any third party organisation without obtaining authority to do so. Some arrangements of this kind are never permissible, for example where they involve:

- a competitor of any Group company; or
- any customer or supplier with whom you deal as part of your role within the Group.

For any other relationship of this kind, you must first disclose it and obtain written approval.

A situation will give rise to the appearance of a conflict of interest where it provides the opportunity for personal benefit, regardless of whether the benefit is in fact obtained.

You should, in the first instance, disclose conflicts and potential conflicts to your line manager. If the line manager has any doubt about whether the situation is permissible or not, then he should seek guidance from higher management and/or local Legal Counsel.

Additionally, in the case of any director of a Group company, disclosure should be made to, and approval sought from, the board of the company at its next meeting, and the decision should be recorded in the minutes.

Potential conflicts must be disclosed in order that management may continue to monitor the situation to ensure that no actual conflict develops.

It is recommended that a Group company's Legal Counsel or Company Secretary take responsibility for maintaining its conflict log.

A corporate opportunity means any business opportunity which properly belongs to the Group or any Group company.

Working for or on behalf of a third party organisation includes taking on a second job, serving as a director or consultant, or otherwise performing services for any organisation outside the Group, including any charitable or other not-for-profit organisation.

This does not apply to any unpaid voluntary work which you may undertake in your own time, provided that it does not interfere with your duties and responsibilities to the Group.

It is not possible to list all situations or relationships which may give rise to a conflict of interest, or the appearance of one, so each situation must be evaluated on its individual facts. However, examples of situations where conflicts of interest may arise, and the principles which should be applied, are given below.

Employees must disclose any material financial interest in any competitor, supplier, customer or other business with which the Group or any Group company has significant business dealings.

Employees may not hold any material financial interest in a supplier, customer or other external business if they have any involvement in the Group's dealings with that business or supervise anyone with such involvement.

Save as may be expressly permitted in writing, no employee may hold a material financial interest in any business the activities of which are:

- in direct competition with the Group or any Group company; or
- otherwise against the interests of the Group or any Group company.

The activities of employees' close relatives can sometimes create conflicts of interest.

Employees should disclose any situation where a close relative works or performs services for, or has a material financial interest in, any competitor, supplier, customer or other business with which the Group or any Group company has significant business dealings.

No employee should have any business involvement with a close relative or with any business for which a close relative works or in which a close relative holds a material financial interest.

No employee should ever be in a situation where they have the ability to hire, supervise, affect terms and conditions of employment, or influence the management of any close relative. A 'material financial interest' means any financial interest which might influence, or appear to influence, your judgment. It does not include publicly traded mutual funds, index funds and similar pooled investments, where the individual investor has no say in which investments are included.

You may be permitted to retain a financial interest in a competitor, provided that:

- the interest was owned prior to your employment in the Group;
- the matter was disclosed in writing to your employing company prior to your appointment; and
- the employing company has not objected.

The prior ownership of any such interest by any director of a Group company must be reported to its board and noted in its next board meeting's minutes.

A 'close relative' is someone with whom you have a close family or personal relationship such that it could give rise to a conflict of interest in the situations described. It includes any spouse, partner, parent, stepparent, child, step-child, sibling, step-sibling, nephew, niece, aunt, uncle, grandparent, grandchild (and any such relationships arising by marriage).

If you work within the same Group company or business unit as a close relative, you should disclose the relationship to your line manager.

Where there is a reporting relationship, direct or indirect, between two close relatives working in the same Group company or business unit, management should take steps to ensure that neither has any managerial influence over the other.

In any case where two close relatives work within the same Group company or business unit, the position should be kept under review by management in order to ensure that there is no possibility of unfairness or undue influence arising in the course of either employee's work.

# Bribery and Corruption

Corruption can cause distortion in markets and harms economic, social and political development, particularly in developing countries. It is therefore wholly unacceptable for Group companies and employees to be involved or implicated in any way in corrupt practices.

Group companies and employees must ensure that:

- they do not, directly or indirectly, offer, promise or give any gift, payment or other benefit to any person for the purposes of securing any improper business or other advantage;
- they do not, directly or indirectly, solicit, accept or receive any gift, payment or other advantage from any person in return for providing any improper business or other advantage; and
- their activities do not otherwise contravene any applicable anti-corruption measures.

An 'improper business or other advantage' means something to which there is no legitimate entitlement and which would not be received but for the bribe, for example a tax concession or the award of a contract.

Group companies and their employees are prohibited from making facilitation payments (directly or indirectly) where this would be in breach of any applicable law.

Where such payments are not prohibited by law, they are in any event strongly discouraged and Group companies should strive to minimise and, wherever possible, eliminate them.

Employees should, wherever practicable, seek legal advice before making any facilitation payment (or otherwise notify their local Legal Counsel as soon as possible after the payment is made).

Group companies and employees must take steps to ensure that improper payments are not offered or made, or solicited or received, on their behalf by third parties.

Bribery is a common form of corruption. Broadly speaking, a bribe is any gift, payment or other benefit to which the recipient (or intended recipient) is not legally entitled and which is offered in order to secure an improper business or other advantage. A bribe need not be paid: it is sufficient that it is solicited or offered.

Virtually all jurisdictions have enacted specific legislation making it a criminal offence to offer or pay a bribe to any public official and many also make it a criminal offence for bribes to be offered to or accepted by employees or agents of private bodies, such as companies. In addition, the anti-bribery laws of many countries have extra-territorial effect, meaning that it is a criminal offence for nationals of those countries to bribe officials in other countries.

Facilitation payments, sometimes called 'speed' or 'grease' payments, are generally defined as small payments made to secure or speed up the performance by a low-level official of a routine or necessary action to which the person making the payment already has legitimate entitlement.

The laws of some countries make it a criminal offence for their nationals to make facilitation payments abroad. So, for example, employees who are UK nationals (and Group companies incorporated in the UK) must never make, authorise or procure facilitation payments anywhere in the world, as to do so would be illegal under UK law.

Group companies can be held liable for the wrongful acts of third parties engaged to act on their behalf. Accordingly, you should always be diligent in selecting contractors, agents and consultants and in monitoring their activity.

The following are examples of corrupt or potentially corrupt activity which you should never engage in:

- offering or making an unauthorised payment, or authorising an improper payment (cash or otherwise) to a local or foreign official, or any related person or entity;
- attempting to induce a local or foreign official to do something illegal;
- 'turning a blind eye to' or failing to report any indication of improper payments or other inducements;
- offering or receiving any gift, payment or other benefit in relation to obtaining business or awarding contracts;

- establishing an unrecorded fund, such as a secret cash account or 'slush' fund, for any purpose;
- doing anything to induce or facilitate someone else to breach this Standard or ignore any violation;
- permitting an agent or representative engaged on behalf of any Group company to take improper actions.

If in any doubt, or if more detailed advice is required, please contact the CFO.

# Entertainment and Gifts

The exchange of entertainment and gifts with business partners can build goodwill in business relationships and, within limits, is perfectly acceptable. However, some gifts and entertainment can create improper influence (or the appearance of improper influence), and might even be seen as bribes.

Group companies and employees must not actively solicit or demand any form of entertainment or gift from any person or organisation outside the Group.

Group companies and employees are permitted to offer or accept business entertainment and gifts without prior approval, provided that the entertainment or gift in question is:

- modest;
- appropriate and consistent with reasonable business practice; and
- permissible under all applicable laws.

The following are examples of entertainment and gifts which are usually acceptable without prior approval:

- Occasional drinks and meals.
- Occasional attendance at sports, theatre and other cultural events.
- Gifts of a token or modest amount.

Some types of entertainment and gifts are never acceptable.

These are:

- Any gift or entertainment that is illegal or prohibited by the other party's organisation.
- Gifts or entertainment involving parties engaged in a tender or competitive bidding process.
- Gifts or entertainment which may have, or may be seen as having, a material effect on any business transaction which has been, or which may be, entered into by any Group company.
- Any gift of cash or cash equivalent.
- Anything that is offered as a quid pro quo (offered for something in return).
- Any inappropriate entertainment.

For any entertainment or gift that falls into neither category above, employees should seek prior written approval from their line manager, and simultaneously notify it to their Company Secretary or Legal Counsel.

This includes:

- Any gift valued at more than the applicable local limit (in the UK, £250 from one source in any one calendar year).
- Any business entertainment involving overseas travel and/or overnight accommodation in excess of two nights.

Group companies should maintain a gifts register, in which any gifts notified and retained as property of the company should be recorded.

There are no restrictions on employees accepting entertainment or gifts offered or provided by the Group or any Group company.

In determining whether a gift or entertainment is appropriate and consistent with reasonable business practice, you should consider the following factors:

- Intent: Is the intent only to build or maintain a business relationship or offer normal courtesy, or is it to influence the recipient's objectivity in making a specific business decision?
- Materiality: Is it sufficiently modest and infrequent?
- Legality: Is it legal both in your country and the country of the other party?
- Transparency: Would you be embarrassed if your manager or colleagues or anyone outside the Group became aware of the entertainment or gift?

In the UK, gifts valued at £250 or less (from one source in any one calendar year) are considered to be of a token or modest amount. Group companies should provide guidance as to what is an acceptable 'token or modest' amount within their markets, not exceeding £250.

Special care must be taken when dealing with government officials, as many countries do not allow officials to accept gifts or entertainment. If in doubt, seek advice from your local Legal Counsel.

Cash equivalent includes gift certificates, loans, shares and share options.

Inappropriate entertainment means anything that is indecent, sexually explicit, does not comply with the Group's commitment to mutual respect or might otherwise adversely affect the reputation of the Group or any Group company, having due regard in all the circumstances to the local culture.

Your line manager, in consultation with your Company Secretary or local Legal Counsel, will determine what is to be done with any gift in excess of the applicable value limit which is offered to or received by you.

In general, any such gift should be refused or (if already received) returned.

However, where it would be inappropriate to refuse or return the gift (such as where to do so might give serious offence), it may be accepted on the basis that it will become the property of the relevant company, unless the company decides otherwise.

You should never avoid your obligation to report or seek approval for any business entertainment or gift by paying personally for it in circumstances where you would otherwise be required to report and/or seek approval for it.

Group companies should nevertheless ensure that any gift or entertainment offered or provided to employees is legitimate, appropriate and proportionate.

## Political Contributions

Subject to the controls set out below, Group companies may make contributions to political parties and organisations, their officers, elected politicians and candidates for elective office, provided that such payments are:

- made solely for the purpose of influencing the debate on issues affecting the company or Group, and not to achieve any improper business or other advantage (such as to secure a government contract);
- not intended personally to benefit the recipient or his or her family, friends, associates or acquaintances; and
- permissible under all applicable laws.

All such contributions should be:

- authorised in advance by the board of the Group company making the contribution;
- fully documented in the company's books; and
- where required by law, placed on the public record.

The Group recognises employees' rights to participate as individuals in the political process. However, when doing so, employees must take care to:

- make sure that they do so in their own time and using their own resources;
- minimise any possibility of their views and actions being misconstrued as those of any Group company rather than their own; and
- ensure that such activities do not conflict with their duties and responsibilities to the Group.

Because of UK legislation which has extra-territorial effect and a very broad definition of 'political organisation', there are procedures that must be followed when it is proposed to make a contribution to any organisation within the European Union which is engaged in political activity (even if originating from Group companies located outside the EU). In these circumstances, Group companies must (in addition to the steps identified opposite) seek prior approval from the Group Director of Corporate & Regulatory Affairs. If given, approval may be made subject to certain conditions.

When engaging in any personal political activity, you should:

- not use company time, property or equipment; and
- where necessary, make clear that your views and actions are your own, not those of the Group or any Group company.

If you plan to seek or accept public office, you should notify your line manager in advance, discuss with him whether your official duties might affect your work, and co-operate with him to minimise any such impact.

# Charitable Contributions

British Marine recognises the role of business as a corporate citizen and Group companies are encouraged to support local community and charitable projects.

Group companies may make charitable contributions and similar types of social investments, provided that these are:

- not made to secure any improper business or other advantage; and
- otherwise permissible under all applicable laws.

Group companies should not make any charitable contribution unless they have taken steps to verify the recipient's reputation or status as a charitable organisation.

Any charitable contribution or other corporate social investment provided by a Group company must be:

- fully documented in the company's books; and
- where required by law, placed on the public record either by the company or by the recipient.

Group companies should always consider any proposal to make a charitable contribution or similar social investment in the context of their overall strategy for corporate social investment, paying due regard to the Group Strategic Framework for Corporate Social Investment. For further information, please contact your local Corporate & Regulatory Affairs (CORA) department.

In jurisdictions where charities are required to register, Group companies should verify that any charity to which they propose contributing is duly registered.

Group companies should take steps to ensure that their charitable contributions reported through CORA (using the London Benchmarking Group guidelines) for social reporting purposes are consistent with those reported through Finance for financial and statutory reporting purposes.



# Accurate Accounting and Record-Keeping

Honest, accurate and objective recording and reporting of information, both financial and nonfinancial, is essential to:

- the Group's credibility and reputation;
  - its ability to meet its legal, tax, audit and regulatory obligations;
- and
- informing and supporting business decisions and actions by Group companies.

All data that Group companies and employees create, whether financial or non-financial must accurately reflect the transactions and events covered.

Group companies and employees must ensure that they follow all applicable laws, external accounting requirements and Group procedures for reporting financial and other business information.

Group companies must adopt records management policies and procedures which reflect the Group Records Management Policy.

All employees must ensure that they manage their business records in accordance with the applicable records management policy and procedures.

Financial data (eg, books, records and accounts) must conform both to generally accepted accounting principles and to the Group's accounting and reporting policies and procedures.

Group companies and their employees must:

- cooperate fully with the Group's external and internal auditors; and
- make sure that all information held by them which is relevant to the audit of any Group company (relevant audit information) is made available to that company's external auditors.

All transactions and contracts must be:

- properly authorised at all levels; and
- accurately and completely recorded.

All contracts entered into by Group companies, whether with another Group company or a third party, must be evidenced in writing.

All documents prepared by any Group company in connection with sales of its products, whether export or domestic, must be accurate and complete and give a proper view of the transaction.

This applies whether the data is in paper documentation, electronic form or any other medium. Failure to keep accurate and complete records is not only contrary to Group policy but may also be illegal. There is never any justification or excuse for falsifying records or misrepresenting facts. Such conduct may constitute fraud and could result in civil or criminal liability.

You should ensure that you are familiar with your company's records management policy and procedures. If you require further information or guidance, you should contact your local Records Manager.

You should never alter or destroy company records, save in accordance with established records management policies and procedures.

Group companies' books, records and accounts must be in accordance with the generally accepted accounting principles applicable to their country of domicile.

For Group reporting, however, information must be in line with the Group's accounting and reporting policies (UK GAAP) and procedures.

Your obligation to cooperate fully with the external auditors is subject to legal constraints, for example in the case of legally privileged documents

– if in doubt, you should contact your local Legal Counsel. Otherwise, you should respond promptly to any request by the external auditors and allow them full and unrestricted access to relevant staff and documents. Under no circumstances should you provide information to the auditors which you know (or ought reasonably to know) is misleading, incomplete or inaccurate.

If you are responsible for preparing, negotiating or approving any contract on behalf of a Group company, you should make sure that it is approved, signed and recorded in

accordance with the relevant contracts approval process. If in doubt, you should contact your Company Secretary or local Legal Counsel.  
All such documents must be retained (together with relevant correspondence) in accordance with the applicable records management policy for possible inspection by tax, customs or other authorities.

# Protection of Corporate Assets

Employees are responsible for safeguarding and making appropriate use of the Group assets with which they are entrusted in order to do their jobs and meet the Group's business objectives.

Group companies and employees must take care to ensure that Group assets are not damaged, misused, misappropriated or wasted.

Employees should report the abuse or misappropriation of Group assets by others. Theft or other fraudulent activity by employees is liable to result in immediate dismissal and prosecution after referral to the appropriate authorities.

Employees must not use any company equipment or facilities for their personal activities save in the limited circumstances set out below.

Limited, occasional or incidental personal use is permitted of certain company equipment and systems issued to employees for their individual business use, provided that it is:

- reasonable and does not interfere with the proper performance of their job;
- does not have an adverse impact on the performance of company systems; and
- is not for any illegal or improper purpose.

All employees are expected to devote sufficient time to their work to enable them to fulfil their job responsibilities.

Group companies and employees must take care to protect all intellectual property owned within the Group.

Group companies and employees must take care to protect all Group funds, guarding against misuse, fraud or theft. All claims for expenses, vouchers, bills and invoices must be accurate and submitted in a timely manner.

Employees must protect information which may be used to provide access to Group assets.

Group companies and employees must never knowingly:

- damage, misuse or misappropriate the physical assets of others;
- infringe valid patents, trademarks, copyrights or other intellectual property in violation of the rights of others; or
- perform unauthorised activities which adversely impact the performance of third parties' systems or resources.

Group assets include physical and intellectual property, time, proprietary information, corporate opportunity and funds belonging to any Group company, as well as equipment and facilities provided to employees for their individual business use.

You are individually responsible for ensuring that the property that you use or come into contact with as part of your work is not damaged, misused or wasted.

Reasonable personal use includes occasional short personal telephone calls or the equivalent use of e-mail, and occasional personal use of the internet.

Improper uses include:

- engaging in communications which might be considered derogatory, defamatory, sexist, racist, obscene, vulgar or otherwise offensive;
- improperly disseminating copyrighted or licensed materials or other proprietary information;
- transmitting chain letters, advertisements or solicitations (unless specifically authorised); and
- visiting inappropriate internet sites.

For further information, please see the Group Security Policy Statement.

Whilst at the workplace, you are expected to be fully engaged in your work and should not undertake personal activities beyond a reasonably modest level which does not interfere with your job responsibilities.

Intellectual property includes patents, copyrights, trademarks, design rights and other proprietary information.

'Group funds' means any cash or cash equivalent belonging to any Group company, including any company money advanced to you and any company credit cards which you may hold.

You should always maintain the security of any information used to access company property and networks, including building access cards, IDs, passwords and pass codes.

You should always show the same respect to the physical and intellectual assets of third parties that you would expect them to show towards the Group's assets.

# Confidentiality and Information Security

Group companies and employees must protect and maintain the confidentiality of all commercially sensitive information, trade secrets and other confidential information relating to the Group and its business.

No employee shall disclose any confidential information relating to any Group company or its business outside the Group without specific authority from higher management to do so.

Where confidential information is to be disclosed to another party, it should be released only:

- to agents or representatives of a Group company who owe a duty of confidentiality to that company and require such information to carry out work on its behalf; or
- under the terms of a written confidentiality agreement or undertaking entered into with the other party.

If confidential information is to be transmitted electronically, then technical and procedural standards should be agreed with the other party.

Where confidential information is required to be disclosed under the terms of an order of any competent judicial, governmental, regulatory or supervisory body, employees should notify their local Legal Counsel and release such information only with Legal Counsel's approval.

Access to confidential information relating to any Group company or its business should only be provided to those employees who require it for the exercise of their functions within the Group.

No employee may retain on his personal premises any confidential information relating to any Group company or its business without making adequate arrangements to protect the security of such information.

No employee shall use confidential information relating to any Group company or its business for his own pecuniary advantage or for that of a friend or relative (see 'Conflicts of Interest').

Group companies and employees must ensure that they comply at all times with all applicable data protection laws.

Access to personal data should be limited to employees who have appropriate authorisation and a clear business need for that data.

Group companies and employees must not solicit or wilfully obtain from any person confidential information belonging to another party.

Confidential information is any information or knowledge, the disclosure of which outside the Group might be prejudicial to the interests of any Group company.

Examples include (but are not limited to):

- sales, marketing and other corporate databases;
- pricing and marketing strategies and plans;
- confidential product information and trade secrets;
- research and technical data;
- new product development material;
- business ideas, processes, proposals or strategies;
- unpublished financial data and results;
- company plans;
- personnel data and matters affecting the morale of employees; and
- software purchased or developed by any Group company.

Inside information is a particular kind of confidential information which is relevant to the price of shares and other securities in publicly quoted companies. While care should be taken with regard to the treatment of all confidential information, particular care should be taken with regard to inside information, since misuse could result in civil or criminal sanctions against both the Group company and the individual concerned (see 'Insider Dealing and Market Abuse' for further detail).

You should be especially mindful of the risk of unintentional disclosure of confidential information through discussions or use of documents in public places.

For further guidance, please see the Group Security Policy Statement.

Data protection laws govern the handling and processing of personal data and may restrict the extent to which such data may be transferred between different companies and jurisdictions.

Such laws will most commonly apply in the context of personal data relating to employees and customers. If you require further information or guidance, you should contact your local Legal Counsel.

Where Group companies and employees inadvertently receive information which they suspect may be confidential information belonging to another party, they should immediately notify their line manager and local Legal Counsel.

# Competition and Anti-Trust Laws

British Marine believes in free competition and Group companies are therefore required strictly to adhere to what are called 'competition' laws in many countries and 'anti-trust' laws in others – laws that promote free and fair competition around the world.

Competition issues may arise as a result of agreements, arrangements or practices (including mergers, acquisitions and joint ventures) entered into between Group companies and competitors or other third parties, and can also arise from unilateral behaviour where Group companies have market power.

Group companies and employees must ensure that they comply with the competition laws of each country and economic area in which they operate.

Certain types of agreements, arrangements and practices almost always break competition laws. For example, employees should never talk or exchange information with competitors in order to:

- fix prices (including setting minimum or maximum prices or 'stabilising' prices);
- fix terms related to price, pricing formulas, credit terms etc;
- divide up markets, customers or territories;
- limit production or capacity; or
- influence the outcome of a competitive bidding process.

Certain types of restrictions between two players at different levels of the supply chain may give rise to violations of competition laws.

These include:

- re-sale price maintenance provisions; and
- territorial or customer restrictions by which the supplier limits the territories into which, and/or the customers to whom, the distributor may re-sell the supplier's products.

Depending on the country, having a particular percentage share of a relevant market may be indicative of market power, in which case particular obligations may apply. Competition laws usually prohibit a company from abusing its market power. Competitor information may not be gathered through unlawful or improper means, including by:

- theft;
- illegal entry;
- bribery;
- misrepresentation; or
- electronic eavesdropping.

Many countries have laws prohibiting anti-competitive behaviour and these can vary from one country or economic area to another. Some competition laws, for example in the US and EU, may have extra-territorial effect, which means that they can apply even where the conduct occurs outside of the relevant country.

Penalties for violation can be severe. In the EU, for example, fines for anticompetitive behaviour can be 10% of group global turnover while, in the UK and US, individuals convicted of conduct such as price-fixing can receive custodial sentences.

Meetings with competitors, for example through trade associations, can be useful and entirely legitimate. However, anyone attending such meetings must take care to ensure that they do not engage in discussions or activities which would lead to the allegation or appearance of improper anticompetitive behaviour.

It is advisable to maintain a careful record of any meetings with representatives of competitors, and you should always break away from a discussion if you are concerned that it may be, or may be construed as, anticompetitive in nature. In such circumstances, you should subsequently notify the situation to your local Legal Counsel.

Not all agreements with competitors or parties operating at different levels of the supply chain restrict competition, and some which do may have beneficial effects which outweigh their restrictions, for example youth smoking prevention initiatives which are not linked to actual competitive behaviour in the market.

A company with market power is prohibited, or at least limited, in its ability to engage in certain practices, for example entering into exclusivity arrangements, giving loyalty rebates,

discriminating between customers, charging excessively high or low prices, or tying or bundling together different products or services.

In order to compete effectively in the global marketplace, it is necessary to gather information about our competitors. However, we will only do so through legitimate means.

If you suspect that a piece of competitor information may have been obtained improperly or may have been disclosed in breach of confidence, you should check with your local Legal Counsel before using it in any way.

If you have any doubt whether a particular business practice or activity might be in breach of any applicable competition or antitrust law, or if more detailed advice is required, please contact your local Legal Counsel.

# Money Laundering and Anti-Terrorism

Money laundering is the process of concealing the identity of illegally obtained money so that it appears to have come from a lawful source. British Marine does not condone, facilitate or support money laundering.

Group companies and their employees must not:

- engage in any transaction which they know or suspect involves the proceeds of criminal activity; or
- otherwise be knowingly involved directly or indirectly in any money laundering activity.

They must pursue practices directed towards ensuring that their activities do not inadvertently contravene any relevant money laundering legislation.

Group companies are required to adopt and maintain procedures designed to:

- minimise the risk of inadvertent participation in transactions involving the proceeds of criminal activity;
- detect and prevent any dishonest involvement in money laundering activity on the part of their employees; and
- support employees in identifying circumstances which ought to give rise to a suspicion of money laundering activity.

Group companies must ensure that their existing customer approval and “know your customer” procedures are sufficient to provide comfort, as far as possible, that their customers are not involved in any form of criminal activity.

Employees should promptly refer suspicious transactions or activities by any customer or other party with whom they are dealing to their General Manager or Head of Function and local Legal Counsel.

Cash payments in excess of €15,000 (or its equivalent in any alternative currency) must not be accepted by Group companies in the EU in any single transaction or series of linked transactions.

Group companies and their employees must:

- ensure that they do not knowingly assist in the financing of, or otherwise provide support for, terrorist activity; and
- pursue practices to ensure that their activities do not otherwise inadvertently contravene any relevant anti-terrorism measures.

Group companies must adopt and maintain procedures and controls designed to prevent inadvertent breach of antiterrorism measures.

Most jurisdictions impose laws making it a criminal offence to engage in money laundering activity. Generally speaking, such laws make it an offence for any person or company to engage in transactions involving assets which they know or suspect are derived from criminal activity.

Penalties for breach of money laundering laws can be severe (including substantial fines and/or imprisonment) and can attach both to individuals and to corporations. In essence, the more effective a company’s procedures are at detecting and preventing money laundering activity, the less likely it is that the company will be liable for prosecution as a result of its employees’ activities.

Few Group employees will ever personally be in a position to infringe money laundering laws. However, you should be conscious of situations which ought to give rise to a suspicion of possible money laundering activity. These include (but are not limited to):

- payments made in currencies other than those specified on the invoice;
- payments made in cash or cash equivalents, in particular where the sum involved is substantial;
- multiple payments from different sources in satisfaction of a single invoice;
- payments to or from an account other than the normal business relationship account;
- requests to make an overpayment;
- payments made by, or requests to supply goods to, someone not a party to the contract; and
- requests to supply goods to a location other than the most proximate branch/office or to adopt an unusual shipping route.



Group companies located outside the EU are, in any event, encouraged to avoid accepting cash payments where the sum involved is substantial.

Terrorist groups are increasingly using legitimate businesses to generate revenue for their networks and activities. Such businesses may range from retail outlets to distribution or financial service companies.

Group companies' anti-terrorism controls should include checks to ensure that they do not deal with any entity which is proscribed, by reason of a known or suspected terrorist association, by any applicable list published by a governmental or inter-governmental organisation.

If in any doubt, or if more detailed advice is required, please contact any director.

# Sanctions

Various sanctions regimes exist throughout the world, ranging from comprehensive economic and trade sanctions to more specific measures such as arms embargoes, travel bans and financial or diplomatic restrictions. Economic and trade sanctions impact upon the businesses of our companies by restricting the extent to which they can operate within certain jurisdictions.

Group companies and employees must ensure that they do not knowingly:

- supply their products, or allow their products to be supplied, to any person;
  - purchase goods from any person; or
  - otherwise deal in any way with any person or property in contravention of any lawful sanction, trade embargo, export control or other trade restriction which is applicable to them.
- Group companies are expected to be aware of, and fully compliant with, all lawful sanctions regimes that impact upon their business and to have in place proper controls and procedures to minimise the risk of breaching such regimes.

Group companies should provide training and support to ensure that their staff involved in the international supply and purchase of products, technologies and services are aware of and understand all applicable sanctions regimes.

Employees should notify their local Counsel immediately and before taking any action if their Group company receives any boycott-related requests, whether oral or written and whether specific to a particular transaction or more general in nature.

Sanctions may be imposed by individual countries and also by supra-national organisations, such as the United Nations and the EU.

Some sanctions regimes may have extraterritorial effect. US sanctions, for example, can apply both to US persons (wherever located) and to exports/re-exports of US-origin product and product with US-origin content (whether or not the entity handling the product is a US person).

Serious penalties, including fines, revocations of export licences and even imprisonment, can apply when sanctions are broken.

Examples of sanctions and other trade restrictions include prohibitions or restrictions on:

- exports or re-exports to a sanctioned country;
- imports from, or dealings in property originating from, a sanctioned country;
- travel to or from a sanctioned country;
- new investments and other dealings in a sanctioned country, or with designated individuals;
- transfer of restricted software, technical data or technology by e-mail, download or visits to sanctioned countries; and
- supporting boycott activity (eg, US anti-boycott laws).

The list of prohibited countries and restrictions is subject to change.

Accordingly, if your work involves the sale or shipment of products, technologies or services across international borders, you should make sure that you keep up to date with the rules that apply.

If in any doubt, or if more detailed advice is required, please contact any director.