

The RBS group Code of Conduct



Integrity Matters : Our Code of Conduct



Contents

Personal Conduct and Business Integrity	5
General conduct.....	6
Managing diversity	6
Performance management	6
Personal finances	6
Crime or offence	6
Working for other organisations.....	6
Outside directorships.....	6
Political activity	7
Conflicts of interest.....	7
How will I know if I have a conflict of interest?.....	7
Possible conflicts of interest: Relationships and associations	7
Possible conflicts of interest: Financial opportunities.....	7
Friends, family and work colleagues	7
Anti bribery and corruption.....	8
Gifts and hospitality	8
Gifts and hospitality – offering and accepting.....	8
Recording gifts and hospitality.....	8
Whistleblowing.....	8
Transactions in securities	8
Safety, Health and Wellbeing	9
Accident, incident and ill health reporting	10
Alcohol and drugs	10
No smoking	10
Driving on business	10
Workload and stress	10
Group Security	11
Protecting the Group’s information, assets and systems.....	12
Personal Use	12
Monitoring.....	12
Clear desk.....	12
Records management.....	12
Protecting Group information	12
Privacy & data protection	12
Using customer and employee information fairly	12
Sharing information between member companies of the RBS group.....	12
International data transfers	12
Media relations.....	13
Notifiable events	13
Group security passes.....	13
Financial crime awareness and duty to report suspicions	13
Minimum standards for all Group employees.....	13
Appendix – Purpose and responsibilities	14
Purpose of the Code	14
Responsibility and enforcement.....	14
Compliance with laws, rules and regulations	14

Who this Code applies to. All Group employees are covered by this Code and the Group Policy Framework Policy Standards relevant to your role. So that the highest standards of conduct are maintained, the Group expects contractors and those engaged through external agencies to adhere to the standards set out in this Code. However, this does not create an employment relationship or rights of employment for such individuals.

You have a responsibility to familiarise yourself with this Code and the standards it sets out, including the Group Policy Framework Policy Standards relevant to your role.

Failure to follow this Code. Adherence to this Code in relation to your personal conduct, business integrity, safety, health, wellbeing and the Group's security are crucial to the maintenance of our reputation and the protection of the Group's interests.

Failure to follow this Code of Conduct, including the Group Policy Framework Policy Standards relevant to your role, will be treated very seriously by the Group and may, in the case of the Group's employees, lead to disciplinary action being taken, in accordance with local policy and laws. This could result in dismissal. If you are a contractor or are engaged through an external agency, a breach of the Code may result in the termination of your relationship with the Group.

In any situation in which you are suspected of breaching the Code, the Group may:

- involve external authorities where external regulations have been breached or where local regulations require their involvement
- involve the police if a criminal offence may have been committed.

Further information. If you have any doubt about whether a course of action is appropriate, consult your manager or the specialist functions referred to in this booklet.

Some Countries also have an Addendum document. These are highlighted at the start of relevant sections.

You can obtain details of any Group Policy Framework Policy Standard or any local standards required via Insite, the Group intranet, or your manager.

Summary points

- You are bound by this Code
- Failure to follow the Code may result in disciplinary action, which could lead to dismissal
- If you're in any doubt about what action to take, consult your manager

Legal Information. The Code of Conduct supports the Group's aim to operate in a similar way across the many countries in which it operates and is therefore applicable to staff in all countries. The Code is a high level summary of information and key policies to inform employees of the Group's expectations of their behaviour and practices. It complements the Group Policy Framework, local policy information and the individual's contract of employment (or offer letter where applicable) and is not intended to be a comprehensive manual.

Detailed requirements for each business unit, to supplement the Code, may be found in a separate policy document issued by each unit. The Group is also committed to ensuring compliance with the laws and regulations of the countries in which it operates. Employees must ensure they abide by local legislation and regulations and could face disciplinary action and possible dismissal if they fail to do so. Should local law conflict with the Code, employees must follow local law in line with instructions from their manager. Should any clause in this Code prove to be invalid or unenforceable for whatever reason, it shall not affect the validity of this Code in total. Such invalid part shall be treated as separate from the Code and may be updated or amended without affecting the whole of the Code. If you are unsure of local legislation or the legality of an action, please ask your manager. If you remain uncertain of the position, the matter must be escalated to a manager with the authority to seek legal advice, if necessary.

Personal Conduct and Business Integrity

This Code of Conduct and related policies form part of the terms and conditions of employment of all those employed by the Group and sets standards for those not directly employed such as contractors and agency workers. The following section details the standards of personal conduct required when working with the Group. It is important that you read and understand these standards as we expect them to be maintained at all times. Consult your manager if you are still unsure about the standards expected of you after reading this Code.

General conduct > Managing diversity > Performance management > Personal finances > Crime or offence > Working for other organisations > Conflicts of interest > Anti bribery and corruption > Whistleblowing > Transactions in securities

Personal Conduct and Business Integrity

General conduct

You are expected to comply with the reasonable instructions of more senior employees and to behave professionally and courteously to all colleagues and customers at all times.

You must attend work punctually and inform your manager of any absences as soon as possible in line with local policy.

Personal appearance can contribute to the Group's image and reputation. Therefore you must maintain a professional image at all times observing local dress codes (including wearing uniforms) as applicable.

When attending events outside of work, you may be regarded as a representative of the Group. As such, you must conduct yourself in a manner that maintains the Group's good reputation.

You must also remember you are bound by the Group's Declaration of Secrecy (sometimes known as Confidentiality Agreement) and that this continues to apply if you leave the Group.

In addition to local policies, you must follow all Group Policy Framework Policy Standards relevant to your role. For example, you need to follow the requirements of the Travel & Entertainment Expenses Policy Standard.

For more details refer to your manager, any local policy information and the Group Policy Framework.

Managing diversity

RBS group values and promotes diversity in all areas of recruitment and employment.

The Group will work towards an environment that is based on meritocracy and inclusion, where all employees can develop their full potential, irrespective of their age, belief, disability, ethnic or national origin, gender, gender identity, marital or civil partnership status, political opinion, race, religion or sexual orientation, or any other characteristic protected by applicable law.

For further information refer to any local Dignity at Work policy information or the Group Policy Framework Diversity Policy Standard.

Performance management

The key to a high performing business is linking individuals' objectives to business goals. Performance management is how we define with you what is expected of you, provide the support you need to meet these expectations (including appropriate

learning and development opportunities) and feed back on how well you have performed against them.

Completion of Group Policy Learning (GPL) forms part of your annual performance objectives and your responsibilities under this Code of Conduct. You must complete all GPL modules appropriate to your role.

For further information refer to the Group Policy Framework Performance Management Policy Standard and the 'Your Performance' pages on Insite.

Personal finances

For following countries, please also read the Country Specific Addendum: Brazil, India, Kazakhstan, Poland, Slovakia, Spain, UAE, USA

Where possible you must hold an account for receipt of salary with a Group company.

Working for a financial services organisation places additional responsibilities on you when managing your personal finances.

You must manage your personal finances responsibly and in accordance with any product terms and conditions, which you have agreed.

The Group regards private gambling as a matter for individual discretion. But, any gambling that results in insolvency or financial problems may render an individual unfit for work and may be treated as a serious disciplinary matter.

Any employee concerned about debt or gambling is advised to contact their manager.

Confidential support is available to employees from Lifematters (see Safety, Health and Wellbeing section below) or:
http://www.group.rbsgrp.net/hr5/Your_Wellbeing/Lifematters/default.asp

Crime or offence

For following countries, please also read the Country Specific Addendum: Czech Republic, India, Kazakhstan, Slovakia, Spain, UAE

If you find yourself charged by the police with a crime or offence you must inform your manager.

A crime or offence as far as the Group is concerned is any breach of common law or enacted law.

It is not automatic that you will be subject to disciplinary action as a result of an offence committed outside of work. The following issues will be taken into consideration when making the decision as to what level, or indeed, if, disciplinary action is appropriate:

- Seriousness of offence
- Impact on contractual duties, for example there would be implications for employees who have access to cash and have been found guilty of stealing
- Whether the Group's reputation is likely to be adversely affected as a result of your actions
- Nature of offence and potential impact within the workplace. For instance, an individual guilty of grievous bodily harm could make colleagues feel compromised about their safety.

Human Resources will assist in assessing consequential action as a result of an individual having committed an offence.

Working for other organisations

For following countries, please also read the Country Specific Addendum: China, Czech Republic, Mexico, Poland, Slovakia, Spain, Taiwan

Before undertaking any work with another organisation, you must seek written authorisation from your manager. To gain this authorisation you must submit a letter to your manager outlining the nature of the job, the name of the company you will be working for and the days and hours you are proposing to work.

Factors that will be taken into account when considering whether to grant authorisation will include the following:

- Whether the business activity will involve interests that have the potential to conflict with any aspect of Group business or the duties you are contracted to undertake. For example, this may apply if you wanted to undertake a role within another financial institution
- Whether your involvement in business activities will impact on your ability to carry out the Group duties you are contracted to undertake effectively and safely. For example, a job involving late nights may impair your ability to work effectively in the morning.

Outside directorships

Executive directors and other members of the Group Executive Committee who receive invitations to become non-executive directors must refer the matter to the Group Chief Executive for approval.

All other employees considering external appointments must refer to the Group Policy Framework Employee Directorships/ Committee Memberships Policy Standard.

Political activity

We recognise individuals may choose to become involved in political activities such as standing for national or local government.

However, if you are involved in politics you have a responsibility to make sure this activity is kept entirely separate from your duties and that Group funds and resources are not used for political purposes.

Conflicts of interest

So that you can undertake your job properly, maintain your objectivity and impartiality and ensure that your judgement could not be compromised, you must not put your personal interests, or those of another person with whom you have a relationship, before the interests of the Group. For these purposes, the term "interests of the Group" is taken in its widest sense.

You have a responsibility to act in the interests of the Group and must not misuse your position or any information obtained in the course of your employment, to further your private interests – or those of anyone you have a relationship with.

How will I know if I have a conflict of interest?

If, in the context of performing your duties, it could be suggested that you are acting in your own interests or those of another person with whom you have a relationship, rather than in the interests of the Group, you may have a conflict of interest.

Possible conflicts of interest: Relationships and associations

For these purposes, the term "relationship" is taken in its widest sense – from playing football with a customer, to sharing membership of the same private club or society with a supplier, to forming a close personal relationship with a colleague.

While the Group entirely respects the right of every one of us to form friendships and personal relationships at work, there will be occasions when it will be appropriate to tell your manager about a relationship that may impact on your work by creating a conflict of interest.

Here are some examples of when it would be appropriate to notify your manager of a potential conflict of interest

Here are some examples of when it would be appropriate to notify your manager of a potential conflict of interest

- You're making a lending decision for someone with whom you have a relationship
- You are making a purchasing decision involving external suppliers and you have a personal relationship with a representative of one of the potential suppliers
- You're conducting an investigation or a hearing under the disciplinary procedure in which an employee with whom you have a personal relationship is implicated.

The onus is on you to identify when it is appropriate to inform your manager of any relationship or association that has the potential to create a conflict of interest.

Possible conflicts of interest: Financial opportunities

For these purposes, the term "financial opportunity" covers any opportunity to obtain a financial advantage or make a personal, financial gain that arises or comes to your attention in the course of your employment. This includes opportunities to make use of business information, or to invest privately in a customer's or a supplier's business, or in the Group's business (this does not include acquiring Group securities which are subject to the Group Policy Framework Employee Share Dealing Policy Standard.)

Here are some examples of situations in which information about a financial opportunity could come to your attention, or an opportunity might become available to you:

- You are involved in a transaction or deal relating to the business of a customer
- You are involved in engaging suppliers or in ordering goods for the Group
- You are advising a business customer regarding their financial arrangements

Pursuing financial opportunities arising in these circumstances could compromise you by placing you in a position where your personal interests could conflict with those of the Group. To deal with this, you must take the following steps

If a financial opportunity becomes available to you, and may be a conflict of interest, before taking advantage of it you must ensure that you disclose all the relevant details – in writing – to your manager and to the head of your department or business unit. You must obtain written permission from the head of your department or business unit before taking up the opportunity.

If pursuing a particular financial opportunity is considered inappropriate, or could create a material conflict of interest, permission to take up the opportunity is likely to be refused or may only be granted subject to certain conditions. If an actual or apparent conflict of interest arises, you must handle that in an ethical manner in accordance with this Code.

You must also comply with these procedures if someone you have a close relationship or association with wants to take up a financial opportunity of this type, which they become aware of, or which, becomes available to them, through you in the course of your employment.

For further information refer to the Group Policy Framework Conflicts of Interest Policy Standard.

Friends, family and work colleagues

To protect your personal integrity and to make sure you stay objective, you must:

- Never process any transactions or lending applications for yourself, friends or family
- Never view or access accounts for friends, family or work colleagues unless an appropriate bank mandate authorisation (i.e. power of attorney or equivalent) is in place
- Only ever process work requests from colleagues if this is within the normal responsibilities of your role (e.g. a cashier must not process a loan application)
- Always deal with your colleagues as you would a customer
- Always declare a personal relationship with someone in your reporting structure
- Never employ a relation without appropriate approval from your manager

In addition you should not borrow from or lend money to colleagues on a personal basis

Personal Conduct and Business Integrity

Anti bribery and corruption

For following countries, please also read the Country Specific Addendum: Kazakhstan

You must never offer or accept any bribe or inducement which may influence or appear to influence your actions. Nor must you misuse your position within the Group or the information you gather in the course of your duties to further your private interests or those of anyone else. If you have a concern, please speak to your manager in the first instance.

Gifts and hospitality

Gifts and entertainments must be properly authorised and recorded and not give rise to any conflicts of interest. Local policy may specify acceptable monetary values to aid application of Group policy.

Special authorisation arrangements apply if any gifts or hospitality are planned for any public or government officials.

Gifts and hospitality – offering and accepting

The majority of employees are not authorised to offer Group hospitality – or gifts- to customers, suppliers or other business contacts, or to accept any hospitality offered.

Small gifts – impersonal items of minimal financial value and often of a promotional nature (e.g. a diary) – from customers or suppliers (actual and potential) can be accepted and kept. Other gifts cannot be accepted without approval from your manager.

To avoid causing offence, you should explain to the person offering the gift or hospitality that you are bound by Group policy. On no account should you accept anything that by its nature has the potential to cause reputational damage or embarrassment to the Group. This may include cash, cash-convertible gifts or any payment, favour or inducement that might improperly influence an official transaction.

Where entertaining is essential to your role you may be authorised by line management to offer or accept hospitality. If you are offering hospitality you must operate within your approved budget for hospitality and adhere to the guidelines below.

Hospitality offered or accepted must be appropriate to the Group's business interests and should not be excessive as regards any contact, customer, supplier or other third party.

A common sense approach should be taken as to what is 'appropriate' or 'excessive'.

Recording gifts and hospitality

Group employees are required to record all offers and receipts of gifts or hospitality appropriately. Ask your manager about the duties and recording procedures in place in your business area.

For further information refer to the Group Policy Framework Anti- Bribery and Corruption Policy Standard.

Whistleblowing

For following countries, please also read the Country Specific Addendum: Slovakia

We want to know about any internal behaviour or questionable business practices you feel may be unethical without fear of victimisation, discrimination, dismissal or detriment.

Concerns can be raised by using the Group's Whistleblowing service, Right Call - an independent, free, confidential telephone helpline and web service.

Right Call aims to reduce the Group's risk, potential losses, and possible reputational damage by providing an impartial service. Both phone calls and web reports are managed confidentially by an independent specialist offering a range of language options.

A unique reference number is provided after each call. Those who raise concerns can review their report on the Right Call website by using their reference code and respond to any additional questions relating to their concern.

For further information refer to the Group Policy Framework Whistleblowing Policy Standard.

If Right Call is not available, refer to your Divisional/Local Regulatory Risk team for details of how to raise any concerns.

Transactions in securities

The Group Policy Framework Employee Share Dealing Policy Standard is designed to ensure that any personal dealings in securities by directors or employees are lawful and do not damage the Group's reputation.

One of the key requirements is that you do not deal in securities while in possession of 'unpublished price sensitive information' - often also referred to as 'inside information'.

Working with the Group you may acquire information that, if disclosed, could affect the Group's share price or those of customers, suppliers or other businesses.

If you hold such knowledge you must take particular care not to reveal it to anyone other than properly authorised colleagues.

Improper disclosure or use of share price sensitive information is illegal. The Group will refer all such cases to the police or other competent authorities and dismiss anyone found to be responsible.

If you believe the security of such information is at risk, inform your manager who will escalate the matter as appropriate to the Head of Country Operations/ Business.

Should you require further assistance please speak to your manager or your regulatory risk/compliance function in the first instance.

Safety, Health and Wellbeing

The safety, health and wellbeing of employees and customers is a fundamental responsibility for any business. In addition to the Group's responsibilities, each individual has personal responsibility that applies to all employees working on Group premises and when working elsewhere on Group business.

As an employee, you are required to:

- take responsibility for your own safety and health and others who may be affected by your actions;
- immediately inform management and others who have responsibility for safety and health if you become aware of anything that may affect the safety or health of employees, customers or visitors to our premises;
- adhere to the Group Safety and Health Policy Standard and supporting Standards and guidance whenever you are working on behalf of the Group;
- take responsibility for maintaining your own health and wellbeing.

For further information refer to the Group Policy Framework Safety and Health Policy Standard:

Accident, incident & ill health reporting > Alcohol and drugs > No smoking > Driving on business > Workload and stress

Accident, incident and ill health reporting

All accidents, incidents (including “near misses” and dangerous occurrences which have not caused injury, but which might have under different circumstances) and work related ill health must be reported to your manager.

Managers are required to report all accidents, incidents and work related ill health following local reporting procedures.

Alcohol and drugs

For following countries, please also read the Country Specific Addendum: Kazakhstan

Employees must ensure that the consumption of alcohol or drugs does not impair their performance or pose a threat to the physical or information security of the Group.

The Group recognises that alcohol or drug misuse is a health problem. The Group encourages those with alcohol or drug related problems to seek professional support.

Support for employees who have concerns about alcohol or drug problems is available from Lifematters, the Group’s Employee Assistance Programme. They offer free and confidential advice, telephone support, face to face counselling and online information to help deal with a range of situations, including debt, childcare, relationships, bereavement or dealing with stress.

Lifematters is available to employees and their immediate family 24 hours a day, seven days a week and can be accessed either by phone or online. For details see: http://www.group.rbsgrp.net/hr5/Your_Wellbeing/Lifematters/default.asp

Unacceptable behaviour or performance arising from alcohol or drug misuse may be viewed as a disciplinary matter.

Following investigation, anyone found to be supplying or dealing in drugs will be dismissed and reported to police.

No smoking

It is recognised that smoking seriously damages the health of smokers, and may cause harm and nuisance to non-smokers. Smoking is also a fire risk.

The Group is committed to minimising the risks and nuisance associated from smoking as far as is possible within the workplace.

Smoking is therefore not permitted on Group premises or in Group vehicles used on Group business.

Driving on business

Employees who drive a vehicle on Group business must comply with the Group’s minimum safety standards and meet local regulations and by-laws whether driving an RBS fleet vehicle, privately owned vehicle or corporate hire car.

Workload and stress

Stress is not an illness, but if prolonged or particularly intense it can lead to increased problems with ill health. Workplace stress exists where people reasonably perceive that they cannot cope with what is being asked of them at work. Factors outside the workplace can have an impact on our ability to cope at work.

If you have any concerns about your ability to cope with what is expected of you at work, you should notify your manager as early as possible. If you are finding it difficult to cope with pressures outside work, you are also encouraged to share your concerns with your manager who may be able to provide you with the help and support you need. The Group acknowledges and recognises the importance of identifying and reducing workplace stressors, and also has a framework of policies and guidance to support employees to balance work and home commitments.

In addition, Lifematters offers free and confidential advice. For details see: http://www.group.rbsgrp.net/hr5/Your_Wellbeing/Lifematters/default.asp

Group Security

You and your manager are responsible for making sure that you are familiar with the corporate standards and security standards relating to your work.

Employees subject to professional regulations laid down by the law, regulatory authorities or other Codes of Conduct are also required to comply with these.

The following sections provide an overview of the key aspects of the policies that relate to the Group's security and safety.

Protecting the Group's information, assets and systems > Records management > Protecting Group information > Privacy & Data protection > Media relations > Notifiable events > Group security passes > Financial crime awareness and duty to report suspicions

Group Security

Protecting the Group's information, assets and systems

For following countries, please also read the Country Specific Addendum: Korea, Spain, Taiwan

Information is one of the Group's most important business assets. You must protect the Group's information at all times to avoid misuse and loss. The Group Policy Framework Information Security Policy Standard is designed to tell you how to secure our information and the supporting systems. By protecting information, you:

- reduce the risk of financial crime;
- protect our customers and employees;
- protect our reputation and brand;
- and help fulfil our legal and regulatory obligations.

You are responsible for making sure that you are familiar with the Group Policy Framework Information Security Policy Standard and for the information you handle.

Personal Use

In your role, you are likely to have access to Group information, systems and equipment (including fax, telephone, email, internet and business applications) and you must apply the relevant Group policies. Personal use is permitted provided it is reasonable and is not to the detriment of your role within the Group. You must not share Group information on the Internet whether you are at work or at home (including blogs or on social networking sites).

Additionally you must not make any statements (including any detrimental or derogatory statements) about the Group or its directors and employees to be distributed or published on the internet or social networking websites that could adversely affect the Group's reputation.

Monitoring

The Group monitors how you use email and the internet within the realms of the law. The Group monitors to confirm compliance with policy standards and to detect and investigate unauthorised transfers of data. Other parts of the Group's infrastructure may also be subject to monitoring, spot checks and audit.

Information that is identified during Group monitoring activity may be retained for the duration of any investigation, disciplinary, regulatory, criminal or appeal proceedings.

Clear desk

In accordance with the Group Policy Framework Information Security Policy Standard, you must not leave sensitive information on your desk when you go home at night or during the day where it may be seen by cleaners, contractors or other visitors to our premises.

Records management

Records are very important business assets. The Group is committed to managing its records in a consistent, systematic and reliable manner. Records provide evidence for business activities and decisions are often required to meet legal and regulatory requirements. You must understand the Group Policy Framework Records Management Policy Standard and your responsibilities for creating, using, retaining and destroying records.

Protecting Group information

You are responsible for protecting Group information and equipment either given to you or that you can access. If you are in control or possession of sensitive information you must protect, delete and destroy it in line with the Group Policy Framework Information Security Policy Standard.

Do not email sensitive information outside the Group without authorisation and using an approved security solution. You must not store Group or customer information on removable media such as memory sticks and laptops unless the information (or device) is encrypted.

If you remove confidential information from Group premises or send it to third parties, you must only do so with permission and in accordance with the requirements of the Group Policy Framework Information Security Policy Standard.

If you have approval to use personal equipment, such as laptops or iPads, to access Group systems you must only use the Group approved security solutions to access Group information. You must always comply with the Group's Acceptable Use requirements.

Privacy & data protection

You are responsible for making sure you are familiar with the Group Policy Framework Privacy and Data Protection Policy Standard and for processing customer and employee personal information fairly, lawfully and confidentially.

Using customer and employee information fairly

In addition to our duty of confidentiality, you must process customer information fairly and lawfully.

You must not use customer or employee information for purposes that they would not reasonably expect or which could be harmful to them. Changes to customer and employee information must be made without delay (or on a specified later date) in accordance with their instructions. You must comply with any request from a customer or employee for a copy of their information by contacting your Divisional Privacy Officer without delay.

Sharing information between member companies of the RBS group

RBS group is made up of many different companies (legal entities). The law does not differentiate between sharing within a single group of companies and sharing with third party companies.

To ensure such sharing is fair and lawful, you must seek advice from your Divisional Privacy officer and your Divisional Legal team before sharing customer or employee information with other RBS group member companies.

International data transfers

We are a global organisation with businesses in many jurisdictions, some of which have very strong privacy, data protection, banking secrecy or confidentiality laws.

Some international transfers, particularly of employee data require prior regulatory (and Works Council) approval. From within the EU, there are restrictions on transferring personal information to non-EU jurisdictions.

To ensure all international data transfers are fair and lawful, you must seek advice from your Divisional Privacy officer and obtain relevant legal guidance before making the transfer.

Media relations

All media enquiries relating to the RBS Group should be referred to your division's media relations team or the Group Media team who are the main point of contact for all media matters. For details of who to contact please refer to your manager or check online: <http://www.rbs.com/media/contact.ashx>

Any member of staff who is trained to act as a spokesperson for their business must consult with the media relations team before communicating with the media on any specific instance unless otherwise cleared.

Employees must not be drawn into discussing Group business or any matters that might reflect on the Group's good name. In particular, employees must not make any personal, financial or political comment.

If in doubt, contact your division or relations team or mail: mediarelations@rbs.co.uk.

Notifiable events

A notifiable event is when something happens that could cause damage to the Group by adversely affecting our customers, our finances or our reputation.

Notifiable events could arise from a wide variety of situations, including:

- a fraud against any part of the Group
- a failure to comply with a regulation or law applicable to the Group
- a breach of security systems errors in the processing of transactions
- a breach of customer confidentiality.

Every employee of the Group, at whatever level, must advise their manager when they become aware of such situations. The guiding principle is „no surprises’ – if in doubt, always tell your manager.

Employees should familiarise themselves with the procedures within their own businesses for escalation and reporting of events.

The Group Notifiable Event Process (GNEP) builds on these divisional or

business level processes to ensure that the appropriate people in the Group are advised, on a consistent and timely basis, of notifiable events, according to the severity of their impact on the Group.

For further information refer to the Group Policy Framework Operational Risk Event & Loss Data Management Policy Standard.

Group security passes

If you are supplied with identification and access passes these must be worn visibly when on Group premises. You are also responsible for the safekeeping of your security passes.

Where visitors to multi-occupied premises are issued with identification passes they must be worn for the duration of the visit. Group hosts are responsible for making sure that visitors are accompanied and that any access given to Group premises and information is appropriate.

If you see someone who is not wearing a pass, challenge him or her. Contact their host for verification if they are an unaccompanied visitor.

For further information refer to the Group Policy Framework Physical Security Policy Standard.

Financial crime awareness and duty to report suspicions

All employees should be aware that they might be personally liable for failing to adhere to the Group's policy (and associated guidance and procedural materials) on:

- sanctions and terrorist financing compliance
- money laundering prevention.

This liability may extend to disciplinary action, a fine, imprisonment (or all three) if found guilty of breaching the relevant legislation.

For more information please refer to your manager, your local regulatory risk or compliance manual or the Group Policy Framework Sanctions, Fraud Prevention or Anti Money Laundering

Policy Standards.

Minimum standards for all Group employees

All Group employees must be aware of the need to report to the appropriate specialist department any instances where they have a reasonable suspicion that a customer relationship:

- is being established or operated in relation to a suspected person such as an individual linked to terrorist financing
- or might involve any aspect of money laundering or fraud.

All staff must be aware of their individual responsibility to prevent and detect fraud within the group. All fraud or suspected fraud incidents, covering both internal and external attempts, regardless of value and whether successful or not, must be reported by staff at the earliest opportunity to the relevant specialist fraud unit for onward escalation. Not only will this assist in adhering to local regulatory requirements, it will also maximise recovery opportunities.

Employees must be aware at all times of their responsibility for ensuring that the Group does not act in breach of its stated policy and should ensure (through their manager) that they are in receipt of regular adequate training to maintain this awareness.

Local provisions apply to varying degrees under local law in every jurisdiction that we are represented in. Accordingly, all employees must ensure that they comply with local law as well as Group policy on sanctions, terrorist financing and money laundering prevention. If you have any concerns you should inform your manager, or a more senior manager in your business area. Alternatively contact any of the specialist Group functions detailed in this Code of Conduct.

Appendix – Purpose and responsibilities

Purpose of the Code

Our Code of Conduct is designed to promote:

- honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships
- full, fair, accurate, timely and understandable disclosure in reports and documents that the Group files with, or submits to, our regulators and in other public communications made by the Group
- compliance with applicable laws, rules and regulations including following Group Policy Framework Policy Standards relevant to your role
- prompt internal reporting of violations of the Code to an appropriate person or persons and accountability for adherence to the Code.

Responsibility and enforcement

All Group employees are bound by this Code. In addition standards set out in this Code also apply to all those engaged by the Group, but who are not employees, such as contractors and those engaged through external agencies.

The Group Director, Human Resources will have primary authority and responsibility for the enforcement of this Code, subject to the supervision of the Group Board and the Group Audit Committee.

In cases relating to the Group Chief Executive and Group Finance Director, the Chairman or the Senior Independent Director will exercise responsibility for enforcement of the Code.

If an actual or apparent conflict of interest arises, you must handle that conflict of interest in an ethical manner in accordance with this Code.

Compliance with laws, rules and regulations

We are strongly committed to conducting our business affairs with honesty and integrity and in full compliance with all applicable laws, rules and regulations. No Group employee shall commit an illegal or unethical act, or instruct others to do so for any reason.

No Group employee is authorised to make contact with any regulator unless they are authorised to do so under the Group Relationships with Regulator Policy Standard (Note: This does not impinge on employee rights under the Group's Whistleblowing provisions)

Further information on all of the policies contained within this Code of Conduct can be found on your intranet site or can be obtained from the departments referred to in this document. Your manager will be able to direct you to any manuals and policies referred to in this Code.

The Royal Bank of Scotland Group plc
Registered in Scotland No 45551
Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB

Agency agreements exist between members of The Royal Bank of Scotland Group
Information is correct at time of going to print January 2012.

EN