Code of Conduct Policy

2024

Data classification: Public

The co-operative bank

Ethical then, now and always

Contents

Policy Owner	People
Version:	3.2
Effective Date:	April 2024

Introduction

Working together co-operatively defines our success. Our customer-led Ethical Policy is one of the main reasons our customers choose to bank with us.

We all have a part to play and we are accountable for delivering positive customer outcomes, making a positive difference to society and reflecting co-operative values and ethics in everything we do.

Mutual trust and confidence is the cornerstone of our Bank. This trust and confidence takes a long time to build up and can be lost overnight. Inappropriate or unethical behaviour can damage our Bank's reputation and undo years of hard work. Our Code of Conduct defines the behaviours and conduct that we expect from all colleagues, at every level, in line with all relevant policies and procedures.

The way we work is what sets us apart as a different kind of bank - it demonstrates that we are holding ourselves to account for our ethics, values and our risk management obligations. We believe in and are committed to excellence in Environmental, Social and Governance (ESG), and in doing so we deliver fair customer outcomes.

Scope & Compliance

The Bank Code of Conduct applies to all colleagues. Unless stated otherwise, the Code of Conduct forms part of the Terms and Conditions of employment for all colleagues.

All colleagues have an obligation to follow and act at all times in line with this policy.

Where a colleague fails to comply with any aspect of this policy, it will result in them being managed in line with the Bank's Disciplinary Policy, which may lead to their dismissal from the Bank. Failure to comply with certain aspects of this policy may also lead to civil and/or criminal penalties. Our regulators; the Prudential Regulatory Authority (PRA) and the Financial Conduct Authority (FCA); have established conduct rules for individuals that must be followed by all colleagues:

The 6 individual Conduct Rules:
Rule 1: act with integrity.
Rule 2: act with due skill, care and diligence.
Rule 3: be open and co-operative with the FCA, PRA and other regulators.
Rule 4: pay due regard to the interests of customers and treat them fairly.
Rule 5: observe proper standards of market conduct.
Rule 6: act to deliver good outcomes for retail customers

There are 4 Senior Manager Conduct Rules which apply to people who carry out Senior Management Functions (for example the Chief Financial Officer) and are approved by the FCA and PRA:

The 4 Senior Manager Conduct Rules:
Rule 1: You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
Rule 2: You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system.
Rule 3: You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.
Rule 4: You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.

Purpose

Our Code of Conduct defines how we will demonstrate to all of our stakeholders that our colleagues behave in line with our Ethical Policy and Guiding Values to deliver the right customer outcomes, deliver on our Environmental, Social and Governance commitments, and comply with regulatory requirements. It also helps the Bank demonstrate to its financial regulators that it complies in full with its obligations and takes appropriate attitudes to risk.

The Code of Conduct has four sections:

1. Upholding our Ethical Policy and Guiding Values
2. Good customer outcomes
3. Risk Management
4. Regulation

1. Upholding our Ethical Policy & Guiding Values

The Code of Conduct incorporates the areas of responsibility outlined in our Ethical Policy and Guiding Values. Together, these define the behaviours and conduct that the Bank expects from all colleagues.

Our Ethical Policy has been shaped by customers for over 30 years - it inspires us to make a difference for the benefit of our planet, people and communities. We often ask our customers to tell us about the things that matter to them and want us to take action on, and regularly update our Ethical Policy to reflect this. After listening to our customers, our latest Ethical Policy focuses on what we do for our planet, people, and the community, and our commitments within these spaces.

The Co-operative Bank was founded as part of the co-operative movement back in 1872, but the co-operative values of self-help, self-responsibility, democracy, equality, equity and solidarity are still important to us today. These values have been enshrined in the Bank's Articles of Association. In common with organisations across the co-operative movement, we believe in the ethical values of honesty, openness, social responsibility and caring for others.

We are committed to keeping co-operative principles at the heart of our business and to demonstrating these values through everything we do. Our impact on society goes beyond the people to whom we are providing banking services, as we seek to drive positive social change through our community initiatives and in co-operation with the partners we work with.

We are accountable to our customers on how well we live up to these standards. Everyone who works for the Bank has a responsibility to apply our values to their areas of responsibility and to live up to the expectations of our customers.

Everyone who works for the Bank also has a responsibility to ensure that the way we live our private lives does not bring the Bank into disrepute.

1.1 Our Guiding Values

The way we work sets us apart as a different kind of bank. As colleagues and leaders, we encourage conversations about how we deliver our business strategy guided by our values. Our Values have not been defined in isolation. They are our own words and they stand for who we are and how we work.

1.2 Behaviours

Roles and Responsibilities – All colleagues

You are required and expected to understand and comply with the Code of Conduct. Please use good judgement to avoid the potential for questions to be raised about your conduct. If you are ever in doubt about a course of action – **ask yourself:**

- Is it consistent with the regulators Conduct Rules?
- Is it consistent with our Code of Conduct?
- Is it consistent with our Ethical Policy?
- Is it consistent with our Guiding and co-operative values?
- Is it legal?
- Will it reflect well on me and the Bank?
- Would I want to read this on social media or the press?

If the answer is "**No**" to any of these questions, then the action is not in line with the Code of Conduct and should not be taken.

You should take responsibility to challenge others if they're not operating in line with the Code of Conduct. If necessary, escalate to a manager or contact the Concern at Work helpline. If you have any questions about the Code of Conduct, or you feel there is a conflict between the policy and any legislation, or local practices, please talk to your leader.

If you are uncertain you should always seek guidance. The Code of Conduct is designed to capture many of the situations that you are likely to encounter, but cannot address every issue or circumstance. You can seek guidance from the following:

- Your leader
- Bank Trade Unions (for colleagues who are members)

You must take responsibility to read, understand and comply with the Code of Conduct, and complete the required mandatory training.

Roles and responsibilities – Leaders

In addition to your responsibilities as an individual colleague, as a leader you should act as a role model of the behaviours expected from your team as they will look to you to see what behaviour / conduct is acceptable, and what isn't.

As a leader you should make sure you understand any aspect of the business for which you are responsible and any risks involved in that business. You should take all reasonable steps to ensure that:

- Any aspect of the business for which you are responsible is controlled effectively
- Any aspect of the business for which you are responsible complies with all relevant regulatory requirements and standards
- Any delegation of responsibilities is to an appropriate person and is overseen effectively
- You inform yourself appropriately about the affairs of any aspect of the business for which you are responsible.

You should champion the Code of Conduct by:

- Ensuring that your team understands their responsibilities under the Code of Conduct
- Reinforcing the importance of the Code of Conduct and creating regular opportunities to discuss it in your team
- Ensuring your team complete all mandatory training modules within the required timescales
- Creating an environment where individuals feel able and comfortable to raise concerns at work without fear of reprisals
- Using the Performance Management & Development Framework to measure colleagues on 'how' they achieve their objectives as well as 'what' they have achieved
- Never condoning, encouraging or directing colleagues to achieve business results in a way that could impact on compliance with the Code of Conduct, relevant regulations or the law
- Always acting to stop violations of the Code, relevant regulations or the law by those that you manage
- Checking if your team have questions and concerns - if you are unsure then seek guidance.

1.3 Management of your personal finances

We expect you to manage your personal finances in a way that does not negatively impact on your ability to carry out your role, expose our business to unnecessary risk or lead to your integrity being questioned. The following list is not exhaustive, but examples include:

- You must not borrow money by overdrawing your personal account (outside of pre authorised overdraft limits), without prior authority
- You must not borrow from or lend money to a customer or other employees except in the course of doing authorised business
- You must never put yourself in a situation where you are financially reliant upon the outcome of a bet or financial speculation.

If you are experiencing any sort of financial difficulty, we have a number of sources of help, advice and support available. It's always a good idea to seek help as early as possible.

1.4 Policies

We have a range of policies and guidance documents that provide specific details on what is expected of you in relation to your conduct. A summary of the points relating to particularly relevant topics is detailed below. Unless stated otherwise in these documents, these policies do not form part of a colleague's contract of employment. This list is not exhaustive and it is each colleague's responsibility to ensure they are familiar with the relevant policies and guidance applicable to their business area.

Diversity

The concept of diversity encompasses acceptance and respect. It means understanding that each individual is unique, and recognising our individual differences. These differences include, but are not limited to: gender, pregnancy and maternity, ethnicity, culture, age, physical and mental ability, sexual orientation, gender identity, religion or belief, marital and civil partnership status, education and those with a caring responsibility.

The Bank promotes equality of opportunity and aims to create a workforce that is representative of our society, knowing that embracing difference enhances the capability of The Co-operative Bank. We will celebrate diversity in all aspects of our business. We will seek to create a genuinely inclusive workspace, which embraces similarities and differences at the individual.

We recognise the need to support the unique and diverse needs of our customer and community base.
We expect all colleagues, our suppliers and partners to actively support us in achieving a diverse and inclusive culture and to be able to demonstrate this.

For further information please see the Diversity and Inclusion Policy.

Bullying & Harassment

This Policy is designed to develop a work environment in which bullying, harassment, discrimination and victimisation is unacceptable, and enables colleagues to have the confidence to challenge inappropriate behaviour without fear of reprisal, allowing concerns to be discreetly, thoroughly and impartially investigated.

For further information please see the Bullying & Harassment Policy.

Social Media guidelines

You are expected at all times to maintain the highest standards of professionalism and integrity in your communication with colleagues, customers, clients and the public.

With online social networks, the lines between our public, private, personal and professional lives can get blurred. If any part of your social media or online footprint identifies you as a Bank colleague, you need to consider how both you and the Bank could be perceived by others. Remember that opinions, comments, and actions can be open to misinterpretation.

If you choose to discuss work, be sure that all discussion is consistent with our behaviours and values. Always make it clear that your views are your own and are not representative of the Bank. If in doubt, it is probably better to avoid discussing work.

How you communicate using social media, and how you talk about the Bank both in and out of work has the potential to impact negatively on the Bank and its reputation. Never make comments or reproduce any material which may be considered unacceptable, distasteful, discriminatory, derogatory, obscene, offensive, libellous, illegal or that incites racial hatred.

Dress Code

Wearing clothes that make you feel confident and professional is a proven way to enhance your work mind-set and productivity.

We encourage cultural diversity and want to ensure colleagues feel comfortable in their attire choices aligned with guidelines outlined to maintain our high professional standards. In all situations clothes should be well-fitted, clean and in good condition.

We have an inclusive approach, embracing diversity where all colleagues can dress in a business casual manner consistent with their identity or expression, including all styles and textures of hair or headscarves within the workplace. We should dress with purpose, in a business appropriate way, for our day. This should ensure we take into account the expectations and interests of those we're interacting with (our colleagues, customers and communities including any site visitors including our regulators) as well as health and safety considerations.

It is important to ensure that you comply with the Dress Code and present yourself at work in an appropriate manner. For further information please see the Dress Code Policy.

Concern at Work (Whistleblowing)

If you have a genuine and work related concern regarding:

- A criminal offence, e.g. fraud
- Someone's health and safety being in danger
- Risk or actual damage to the environment
- A miscarriage of justice
- The Bank breaking the law or regulation
- A breach of the Bank's internal policies or procedures (including the Code of Conduct)
- Behaviour that harms or is likely to harm the reputation or financial well-being of the Bank; or
- If you have a belief that someone is covering up any of the above wrongdoing, take responsibility and raise your concerns. You can raise your concern at any time about any incident that has already happened, is happening now, or you believe may happen in the near future. Concerns can be raised via the following options:

- **Option 1**: Raise the matter with your leader or, if this is not appropriate or you feel uncomfortable doing so, to a senior leader within your department or directorate. This may be done verbally or in writing
- **Option 2**: By getting in touch with the Major Investigations Team via confidential routes
- **Option 3**: Where appropriate, contact the Bank's appointed Whistleblowers Champion
- **Option 4**: In addition, or where you feel you are not able to raise a matter internally, you are entitled to contact our regulators directly:
- **Financial Conduct Authority** on 020 7066 9200; at whistle@fca.org.uk, or at Intelligence Department (Ref PIDA), Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN

- **Prudential Regulation Authority** on 020 3461 8703; at whistleblowing@bankofengland.co.uk; or at : Confidential reporting (whistleblowing), IAWB team, Legal Directorate, Bank of England, Threadneedle Street, London, EC2R 8AH.

All concerns will be treated sympathetically and in the strictest confidence.

Please see the Concern at Work Policy for further details.

Alcohol and Drugs

You must not attend work if you are under the influence of alcohol or drugs, including prescription medication, to the extent that your judgment, behaviour or ability to carry out work duties is affected. Where you are required to drive for work purposes you must ensure that it is legal to do so. Where you have been prescribed medication that you believe may affect your ability to do the job safely and efficiently, then you should discuss the situation with your leader as soon as possible. For further information please see the Drugs and Alcohol Policy.

Security

You must always display your security pass when on Bank premises and if you are comfortable to do so, challenge colleagues who are not displaying a pass. If you observe suspicious behaviour then please report the matter to your manager or member of the security team. When accessing your floor, please do not allow colleagues to 'tailgate' and gain unauthorised access to the floor.

Search Policy

The Bank has a duty to protect both the organisation and colleagues from criminal activities such as any theft of the company's property or property belonging to another, or the possession or supply of illegal substances. At any time you may be asked by a leader or a member of security staff to empty your pockets, baggage (both personal and that owned by the company) or provide access to all work areas including, but not limited to, desks, lockers and cabinets or to allow a search of any company vehicle or private vehicle parked on Bank premises.

Use of mobile devices

The use of personal mobile phones and other devices during your working hours should not interfere with you carrying out your role. If your business area has specific guidelines on the use of mobile devices you must familiarise yourself with them.

Colleague Welfare

If you are concerned about the welfare of one of your colleagues (both inside and outside of the workplace) then you should speak with your leader.

Working from Home

The Bank supports colleagues to work from home where operationally possible. If you are working from home, we will provide and maintain all equipment and materials necessary. You must complete a risk assessment to assess appropriate equipment and

work space, and ensure you take adequate rest breaks. It is your duty to ensure that proper care is taken of all equipment and materials provided by the Bank, and to ensure that you and all other people in your household are not endangered by the work activities undertaken at home.

You will come into an office or branch location when necessary for the effective delivery of your role. You will adhere to all policies and procedures as you would if working in an office or branch, and must engage with all regular performance, development and support processes in the same way.

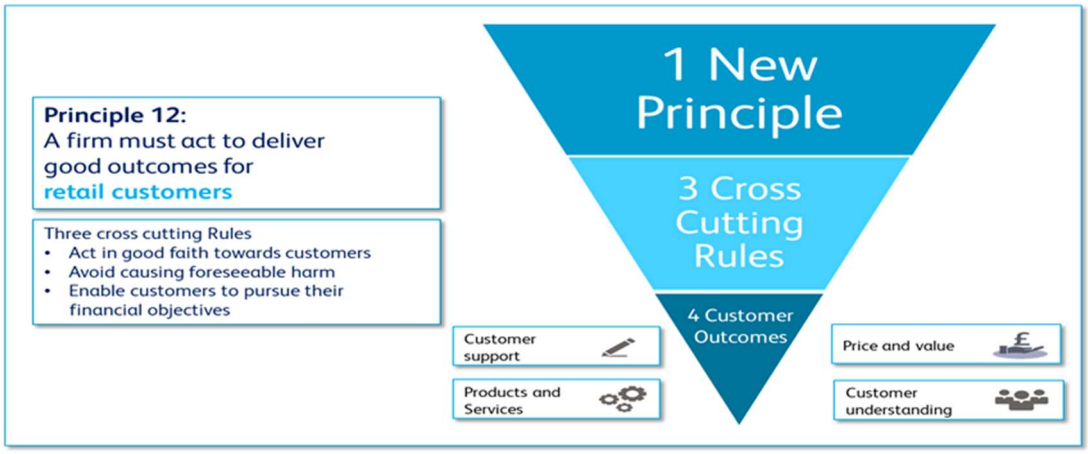
Whether at home or on Bank premises, you are expected at all times to maintain the highest standards of professionalism and integrity in your communication with colleagues, customers, clients and the public.

Be mindful of your home working environment and that others may overhear your conversations. You may be sharing your home working space with other family members or friends. Do not discuss information which is confidential or highly confidential within earshot of others. Try to hold conversations where others are less likely to overhear you and position your screen where it is less likely to be overseen. Always ensure confidential and highly confidential data is entered securely into the appropriate application from a Bank device and never written onto paper, and never write down passwords, card, account numbers or user credentials on paper.

2. Good Customer Outcomes

2.1 Consumer Duty

The FCA has introduced the Consumer Duty, which is designed to increase the current level of consumer protection in the retail financial services market. The Consumer Duty signals a "paradigm shift" in the FCA's expectations of firms and impacts all areas of our business. It has moved from a rules-based, prescriptive approach to a more data-led, outcomes focussed approach where it will require firms need to consider the impact of their products and services on their customers.



When you're looking at existing arrangements or making changes to them (whether they relate to products, services, processes or systems capability) you can ensure that your approach is aligned to the Consumer Duty by asking yourself the following key questions:

1. What are the outcomes we want to deliver to our customers?

1. What are the outcomes we want to deliver to our customers?

   Our starting point should be what does "good" looks like and then we need to think about how we deliver that
2. How do we know we are delivering those outcomes to our customers?
   We can evidence these outcomes through data, QC, QA, and customer feedback
3. What harm could we cause to our customers if we do not deliver those outcomes?
   Think about what could go wrong for our customers and what harm this could cause. Consider if different groups of customers, e.g. those that are vulnerable, will suffer worse outcomes
4. What do we need to do to prevent harm?
   Putting the right controls in place and then acting if harm does happen

2.2 Conduct Risk

Conduct Risk is defined as the risk that the Bank's behaviours, products or services will result in poor outcomes or harm for customers.

Conduct Risks may exist in any aspect of the way business is conducted.

"Conduct Risk" is in simple terms about putting the customer at the centre of what we do to achieve good customer outcomes. It is essential that you consistently act in line with this Policy and the Bank's Guiding Values to ensure:

- All decisions you make aim to deliver good customer outcomes
- You take personal responsibility for delivering good outcomes at all times, with our direct and indirect dealings with our customers
- We put things right if we make mistakes.

Whatever your role, you play a part in achieving good customer outcomes. You should think about whether:

- You put the customer first
- You put yourself firmly in our customers' shoes before you act
- You take into account the characteristics of the customers – including any characteristics of vulnerability and tailor how you communicate with the customer
- You understand how you affect the experience we create for our customers.
- You play your part in ensuring good customer outcomes
- You understand our products and how they operate
- You don't assume to know what our customers want
- You don't ignore customer feedback.

It is important to highlight if you think we are not delivering good customer outcomes. Escalating issues will help identify process improvements or manage risks to customers at an early stage. If in doubt, ask your leader in the first instance or Compliance.

The Bank has a Conduct Risk Policy and Control Standard which set out in further detail what this means. Following these requirements will help you to keep the customer at the heart of how we operate and help us meet the expectations set out by the Financial Conduct Authority. If you are responsible for products, processes or systems you must be familiar with and follow these Policy and Control Standard requirements.

As an employee of the Bank, it is important to be aware that:

- You are expected to act at all times with integrity and honesty in your business and personal dealings to protect the interests of our customers and the Bank
- You are expected to act at all times conscientiously and with due skill, care and diligence when carrying out every aspect of your role as an employee.
- You must not use company property, information, or position for personal gain, or to compete with our business directly or indirectly.
- You should report to your leader any allegations, charges or convictions for criminal conduct, or breaches of financial regulations. Your leader will then be able to take any appropriate steps regarding your employment and/or provide support
- If you believe you have breached a requirement of confidentiality, even if inadvertently, you should raise this with your leader.

3. Risk

3.1 Risk Management

Risk is everybody's business. We should all be fully aware that risks have the potential to damage our organization, both reputationally and financially.

Managing both internal and external risk is essential to enable the Bank to remain financially strong and to achieve its objectives. Risk Management is a planned and systematic approach to identifying, evaluating and controlling risk. There will be frameworks, processes and controls in place within your department that have been agreed to manage risk in the area you work. Colleagues should follow the procedures and control requirements as they are there for a purpose and any shortcuts could expose the Bank to unacceptable risks. However, we do have to think and act differently, and challenge the way we do things and ask ourselves if what we do really drives the right outcomes for customers. Sometimes, this will mean our normal approach is not the right one and you can make a difference by raising this as an exception to policy with your line manager. If you are unclear or would like to know more about how the framework operates or what risks apply to your role, speak to your line manager. Please visit the Risk pages on the intranet for further information.

3.2 Financial crime

Preventing fraud

Every business in the financial sector must take steps to reduce the risk of fraud by colleagues or associated persons, customers or members of the public. Our customers trust us to look after their money and data and to proactively investigate any unusual activity on their accounts. In some areas of the business, to help us prevent financial crime we may ask you not leave personal items such as handbags, mobiles and diaries on or around your desktop, either attended or unattended. At all times, you must strictly adhere to customer identification procedures to ensure customers' money and data are protected.

If you suspect that someone is involved in a fraudulent activity, you must immediately report this to your leader or raise your concerns in the way described in the Concern at Work (Whistleblowing) Policy. Speak to your leader if you suspect any of the following or other suspicious behavior:

- Someone has been approached to give customer account information to unauthorised persons inside or outside the organisation
- A customer's security code and/or SPI (Secure Personal Information) / URN (unique

reference number) have been compromised and could be used to gain funds fraudulently
- A process is not being followed appropriately, which could have implications for a customer or the organization
- Colleague(s) deliberately aid or are indifferent to instances where they know / suspect activity which may be linked to a criminal offence, and they proceed anyway
- Someone is involved in the facilitation of tax evasion.

The Bank may be criminally liable where a specified fraud offence is committed by an employee or associated person, for the Bank's benefit, or if reasonable fraud prevention procedures are not in place.
The Bank has a zero tolerance approach to fraud and in the case of an employee committing an act of dishonesty, then the act will be reported to the appropriate authorities. Fraud is a criminal offence and any colleague suspected of fraudulent activity either as an employee or as customer will be investigated. In addition to an internal investigation, the matter and any potential evidence will be referred to the police for prosecution where appropriate.

Fraud prevention databases have been established for the purpose of allowing employers to share data on their employee fraud cases. We will check details with/against fraud prevention databases. Should investigations identify fraud or the commission of any criminal offence by you when applying for a role or during the course of your time with us we will record details of this on the relevant fraud prevention databases.

This information may be accessed from the UK and other countries and used by law enforcement agencies and by us and other employers (and potential employers) to prevent fraud. If you want to receive details of the relevant fraud prevention databases through which we share information, then please contact HR Support.

Money laundering, terrorist financing, financial sanctions and proliferation financing

Money laundering (ML) is the process by which criminals introduce funds into the financial system, in order to disguise their origins and to create a seemingly legitimate source of money that they can then use for whatever purpose they wish.

Terrorist financing (TF) is defined as providing financial support, in any form, to those who encourage, plan or engage in terrorism. TF can differ from ML in that the source of funds may be legitimate, such as an individual's salary or donations from the public, as well as from illegitimate sources.

Financial Sanctions (FS) are applied by governments or international organisations (such as the United Kingdom, United States, United Nations and the European Union) to exert pressure on regimes, entities, groups or individuals, to seek to change their behaviour. Sanctions comprise a variety of measures including financial restrictions, arms embargoes and trade restrictions.

Proliferation Financing (PF) means the act of providing funds or financial services for use in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons in contravention of a relevant financial sanctions obligation.

All financial organisations are required by law to have appropriate controls to prevent, detect and report money laundering, terrorist and/or proliferation financing and breaches of financial sanctions. If an organisation's products or services are used to launder money or facilitate

terrorist, and/or proliferation financing or we breach financial sanctions the organisation can face legal and regulatory penalties along with reputational damage. The Bank therefore has appropriate and risk based anti-money laundering (AML) counter terrorist financing (CTF), financial sanctions (FS) and proliferation financing (PF) measures, systems, procedures and controls in place to manage these risks.

For colleagues, there are three individual principal offences detailed in the regulations:

- Money laundering or assisting a money launderer
- Tipping off or prejudicing an investigation
- Failure to report suspicions.

As part of your legal obligations as an employee of a regulated financial institution, you must be aware of AML, CTF, FS & PF risks. You have a personal responsibility to report any suspicions that you have of money laundering or terrorist and/or proliferation financing through the Bank's internal reporting processes. To avoid the risk of "tipping off, if you believe that a report has been made, you must not discuss this with anyone except the Bank's AML teams". Additionally, employees must not make funds available to, or deal with economic resources held or controlled directly or indirectly by (or for the benefit of) a sanctions target or person acting on their behalf. Employees must also not say or do anything that may help circumvent financial sanctions.

New colleagues will receive training on the prevention, detection and reporting of money laundering, terrorist and proliferation financing and financial sanctions. Training must be completed on a regular basis by all colleagues. Where specific AML, CFT, FS & PF procedures apply to your role, your leader will discuss these with you, e.g. opening of accounts, processing foreign payments and customer contact roles. This is not an exhaustive list of examples, there are many processes throughout the Bank that require consideration of AML, CTF, FS & PF risks.

If you identify any suspicions of money laundering or terrorist financing taking place, or being attempted, you must report this immediately through the internal reporting process. For further information please refer to the anti-money laundering pages on the Bank intranet.

3.3 Business Confidentiality and Price Sensitive Information

All staff are subject to standard confidentiality clauses which mean you must not, as a general principle, copy, share or discuss confidential matters about the Bank or its customers. You should also take steps to keep such information safe.

If you are in possession of confidential information you must not share this information externally and you should only do so internally with others that you know need that information to perform their job.

Examples of confidential information include:

- **Strategic deals** – e.g. if the Bank is about to enter into or amend a significant relationship with a third party supplier that is confidential
- **Customer information** – e.g. if you know something about a company because it, or one of its owners, is a customer (see also "Information Security" section around the protection and use of customer data)
- **Bank financial performance** – e.g. details about the financial performance of the Bank

- **Information impacting staff** – e.g. information about organisational restructures, outsourcing, reward plans

You are not allowed to use or take advantage of this information. To do so would result in disciplinary action and potentially serious regulatory and legal consequences covered by Market Abuse regulations. Market Abuse covers a number of potential offences, the most commonly known is "insider dealing".

Most colleagues, most of the time, will not be in possession of Inside Information about the Bank, its suppliers, its corporate customers or counterparties, but if you are you must not share that information without good reason or knowingly take decisions (on shares, debt or other types of investment) to buy or sell based on information you have that is not public.

If you have any doubts or you feel that you may have inadvertently breached confidentiality you should speak to your leader or a colleague in Risk for further advice.

All colleagues (including each Director and any contractors of the Bank), who are planning on making personal investments in securities, (including but not limited to debt, equity instruments such as shares or "over the counter" products such as spread bets in stocks), must adhere to the requirements of Bank's 'Personal Investment Dealing Procedure'. This procedure stipulates the expected standards of practice and the pre-clearance procedures to be followed, in respect of all personal investments. It is essential that individuals familiarise themselves with the policy prior to undertaking personal investments in securities, as failure to comply could ultimately lead to their dismissal from the Bank.

3.4 Conflicts of interest

In general terms, a conflict of interest exists where a person's private interest interferes with, or could interfere with, the interests of our business (e.g. influencing us to use a supplier that is owned by a family member or friend) or its customers. We want to protect you from having your integrity questioned. Below are some example types of conflict of interest. Ask your leader (or any other member of the management team) if you are concerned about these or any other potential or actual conflict of interest:

- Your account* – To prevent your actions being questioned, you must not view, access or carry out any transactions on your own accounts other than as a customer using normal customer channels such as internet banking.
- Friend and family member accounts* – Do not view or carry out transactions on the accounts of family members or friends.
- Remember you should not access any customer's records, even if your ID allows you access, unless there is a business need to do so.

*An account is any type of product including insurance policies.

Lending

If you are involved in recommending or approving any credit facility or counterparty limit for a customer and either yourself or a person connected to you (e.g. a family member or close friend) has a significant investment in the customer – you should talk to your leader so they can be satisfied that the approval of credit facilities has not been influenced by the relationship / investment

Relationships at work

This can sometimes cause real or perceived conflicts ofinterest. These are most likely to arise where the parties in the relationship are in a direct or indirect management relationship or are involved in the same activities, processes or controls. If you have a relationship with another colleague, we ask that you let your leader know (to consider the risks) within a reasonable timeframe of any:

- personal relationship that might result in your objectivity or integrity being challenged
- relationships that you form with a colleague with whom you have a management relationship, whether direct or indirect or where you work on the same processes and systems.

Additional or secondary employment, directorships

Written permission via the 'Secondary Employment Request form' is needed before commencing any secondary employment or directorships (even if on a short term career break) to ensure that it will not interfere with your commitments to us or adversely affect any relationships with customers. There are some circumstances where we may refuse permission for example the following situations:

- a conflict of interest may arise, e.g. you will be working for a direct competitor
- the employment is likely to damage your reputation or the reputation of the Bank
- your work performance is likely to be adversely affected – this includes specific regulatory expectations for certain senior roles
- the working arrangement fails to meet the requirements of the Working Time Regulations.

For leaders who are:

- involved in the setting of and awarding of remuneration (fixed or variable)
- have influence over decisions regarding business results which impact their own remuneration
- involved in the Bank's risk adjustments processes,

particular consideration should be given to any conflicts of interest that may arise and they should ensure the correct governance approach is followed to mitigate any conflicts of interest appropriately.

Note: From a regulatory perspective, there are specific systems and controls requirements where a conflict results in or may result in material detriment to customers (whether that is in favour of the Bank, its employees or another group of customers). Most of the time the above examples will not result in material detriment to customers but if they do, or you become aware of any other conflict that does, these should be escalated to your local Risk Manager for inclusion in the Conflicts of Interest log.

3.5 Information security

The protection of customer and colleague information is extremely important to us. It must all be treated as confidential. We don't want sensitive or confidential information to be used in a way that could have a negative impact on a customer or colleague. Imagine how you would feel finding out that a company you trusted to look after your personal information had lost or misused it. Would you be happy about this?

This is why it is vital you understand how you can protect information while working for the Bank. You have a responsibility to handle sensitive and confidential data securely and to not expose our business to the risk of data loss or misuse, and it is important for you to familiarise yourself with our policies and ensure you follow them.

The Bank applies the following classification to data;

Highly confidential: Extremely sensitive information/data that is restricted to a small number of people. Examples of this include encryption keys, merger/acquisition strategies, redundancy plans, board papers, financial results prior to publishing, PIN numbers.

Confidential: Information that the company and its colleagues have a legal, regulatory or social obligation to protect including business and strategic plans, bank account details, personal employee or customer data, third party contracts, telephone recordings.

Internal use only: Information which is not restricted internally but is not approved for general circulation outside the Bank. Examples of this include organisational charts, policy and procedure documentation, internal directory listings.

By taking responsibility for ensuring that confidential data is treated and held securely, you are protecting customers, colleagues and the Bank's reputation. You must ensure that:

- Confidential data is not left on printers, photocopiers or fax machines nor on desks even during short periods;
- Privacy monitor screens are used where necessary and screens are locked whilst you area away from your desk;
- All paperwork is locked away at the end of the working day;
- You never send work emails to a personal email address and management approval is obtained prior to transfer of data. Failure to comply with this will lead to disciplinary action being taken against you up to and including dismissal without notice;
- Attachments are password protected.

For additional guidance please see the Information & Data Risk Policy and its related Control Standard and Procedural Guidance, which also set out the Bank's Acceptable Use guidelines. If you have any concerns about your ability to do this follow these controls or have any suggestions for improvement in your local working area, you should discuss these with your leader.

3.6 Fair practices

You are only allowed to accept a bequest (e.g. to be left something under the terms of a customer's will if you can clearly demonstrate that the customer's wishes were not influenced, in any way, by activities you undertook as an employee of the Bank. If you are found to have exerted inappropriate influence over the customer you will be advised to decline the bequest and formal action will be taken in line with the Disciplinary Policy.

4. Regulation

4.1 Regulatory Compliance

Colleagues must be fully aware of all responsibilities to comply with applicable legislation, rules, and codes of practice or conduct laid by external authorities including the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

Colleagues must be open and co-operative with the FCA, PRA and any other regulators they may have contact with. This includes not obstructing the appropriate reporting of any matters to a regulator by another colleague. To ensure both Board and regulator expectations are met, colleagues must adhere to the Regulator Contact Principles in any dealings they have with the FCA or PRA

If a colleague is in doubt please contact the 'Regulatory Affairs' team to confirm.

4.2 Market Conduct

In addition to the requirements relating to price-sensitive information, colleagues who trade on, or have any interaction with, any markets must observe proper standards of market conduct generally. For example, colleagues must not manipulate or attempt to manipulate a market, such as a stock market or a foreign exchange market, or a benchmark.

4.4 Mandatory Bank Wide Training

The Bank has a responsibility to provide you with core knowledge training which all colleagues must undertake. The process around providing mandatory knowledge training demonstrates to our regulators that as a business we have a robust framework and process in place that allows users to have a sufficient understanding around the financial sector we operate in and the principles that govern us. This is achieved through a curriculum of mandatory training modules that all colleagues must complete at the beginning of their employment and then on an annual basis thereafter or as required.

Your leader will be able to provide you with more information on the process you will need to follow.

Upon receipt of a notification to complete the training, it is important that you complete the mandatory bank wide training within the agreed timescales. If this is not completed, it will have a negative effect on your performance rating.

4.5 Gifts and hospitality

Gifts and hospitality may be offered or received in the normal course of doing business and can enhance business relationships. However offering or accepting gifts or hospitality must never create a conflict between personal interests and professional obligations.

The Bank places monetary limits on the value of gifts and hospitality that you may accept from external individuals and companies. This is to minimise the risk of bribery or perceived bribery, the impact to the Bank, and the reputational damage this could cause.

Money (in all its forms, e.g. cash, cheques or vouchers) must never be offered or accepted as a gift. If you are offered money you must inform your leader. If you are offered a gift or hospitality and the monetary value exceeds the limits set out in the Gifts and Hospitality Guidance, you must notify your manager before accepting the offer.

Details of any offers of gifts or hospitality must be recorded in the gifts and hospitality register whether the gift or hospitality has been accepted or not and include a business justification for accepting or declining any offer. You must be comfortable that the gift or hospitality you are being offered is for a genuine business reason, does not create expectations, and would be appropriate to disclose to our customers. If in doubt, refer to your leader or 2LOD Financial Crime Team for guidance before offering or accepting business gifts or hospitality.

It is never acceptable to offer or accept services, benefits, gifts or hospitality in circumstances in which it may be construed as an incentive to influence a business judgement in your favour or that of a third party. Any breach of these guidelines will be investigated and this may result in formal action being taken in line with the Disciplinary Policy.

For further information please refer to the Internal Fraud and Anti-Bribery and Corruption Control Standard and the Gifts and Hospitality Guidance on the intranet.

4.6 Bribery and corruption

Bribery is the offering, promise of or acceptance of any incentive, gift or advantage for personal gain, corporate gain or a breach of trust. There are four bribery offences under the Bribery Act 2010;

- Bribing – the offering, promising or giving of an advantage
- Being bribed – requesting or agreeing to receive or accepting an advantage
- Bribing a foreign public official
- Where an organisation fails to prevent bribery from being committed.

The Bank must comply with the requirements set out in the Bribery Act 2010. It does not matter whether the offence was committed in the UK or abroad.

The Bank has a ‘zero tolerance’ stance on bribery and corruption. It is never acceptable to offer, promise, give or accept a bribe, unauthorised payment or inducement of any kind. Failure to meet this requirement will result in action being taken in line with the Disciplinary Policy.

The consequences of offering or accepting a bribe or inducement for any colleague or third party acting on our behalf can result in regulatory and criminal sanction, not only for the individual involved but also for the Bank. This could lead to reputational damage to our business and a negative impact on our customers.

If in doubt, you must ask your leader for advice in advance or refer to the Internal Fraud and Anti-Bribery and Corruption Control Standard on the intranet.

4.7 Using office systems

You must always use the office systems in a responsible way and follow any procedures that are in place.

Office systems including computers, telephones, email and internet facilities are provided for the purpose of doing your job. Their misuse can potentially create liability for the Bank and put its reputation at risk. You must not use your system access privileges to view your own product information or data except where you are specifically authorised to do so.

You must keep secret and never loan or share your access mechanisms e.g. user id and password to anyone as you are personally responsible for any actions that take place on your user id.

Limited, appropriate personal use of the systems is acceptable but must not interfere with or disrupt your work activities or those of your colleagues. However all use of the systems, including email, the internet, voicemail and text messages may be monitored and therefore cannot be considered as private. Bypassing or causing compromise of any security mechanisms/ processes, whether physical or electronic, or transmitting confidential data will be treated seriously and may result in you being managed in line with the Disciplinary Policy. It may also be considered a criminal offence.

4.8 Communications

You are expected at all times to maintain the highest standards of professionalism and integrity in your communications with colleagues, customers, clients and the public. These standards apply to communications that are verbal, written and electronic – including but not limited to faxes, email, texts, telephone, voicemail and the internet. Business records and communications often become public and you should always avoid exaggeration, insulting remarks, guesswork or any inappropriate comments, whether in systems or documents.

This also applies to any communications or comments you make outside of work, for example via social networking sites where these have or could damage the reputation of our business. Please also refer to the Social Media Policy for more information.