BankABC

ABC Group
Code of Conduct

Table of Content

1. *About the Code* 4
2. *Our People* 6
3. *Our Clients and the Marketplace* 7
4. *Financial Crime* 9
5. *Data Privacy and Protection* 11
6. *Protecting our Assets* 11
7. *Conflict of Interest* 13
8. *Social Media Guidelines for staff* 14
9. *Relations with Regulators and Auditors* 14
10. *Raising Concerns* 15
11. *Version* 15

Message from the Group CEO

Our vision is to be MENA's leading international bank. In striving to achieve this vision, our Code of Conduct is instrumental to help you to maintain the highest standards of ethical and professional behavior at all times. Ultimately, we rely on your personal integrity to protect our reputation and to ensure the success of our Bank.

At a time when banks are increasingly coming under scrutiny for their ethical conduct, we pride ourselves on always doing business the right way. This Code documents and reinforces such core values for our Bank. It sets out how we should behave with all our stakeholders, including customers, communities, investors and regulators.

It is your responsibility to ensure you understand and comply with both the letter and the spirit of our Code. If you are unsure, please seek advice from your line manager or Unit Head of Compliance.

Dr. Khaled Kawan
Group Chief Executive Officer

1. About the Code

1.1. Introduction

Bank ABC (the "Bank", "Group" or "ABC") is committed to maintaining the highest standards of ethical and professional conduct.

This Code sets out the minimum standards of behavior that are expected across the Group from our employees, directors, senior management and contract and temporary workers (herein referred to as "employees").

This Code is supported by policies and standards that you are also expected to read and understand. It should also be read in conjunction with any supporting procedures and your employment contract.

Where local laws or regulations applicable to your Unit set stricter requirements than those detailed in this Code, you must follow them.

If you have any questions about the Code, seek advice from your line manager or Unit Head of Compliance.

1.2. Our Values

You should display behaviors that reflect our Values in your day to day activities performed on behalf of the Bank. Our Values are:

Client Centric
We are committed to knowing our clients and developing long-term relationships with them, making sure we provide them with superb services.

- Focused on building client relationships at every level
- Responding quickly to our clients, recognizing the importance of speed in today's world
- Maintaining continuous and open dialogue to identify client needs
- Identifying and delivering insights and tailored solutions

Collaborative
We work together as one team across our international network providing a superior client experience.

- Harnessing our international network footprint
- Focused on a cohesive team working across boundaries
- Putting our client's needs for cross-border service before our individual targets
- Finding new ways to conduct our business and streamline operations

Consistent
We are trusted to deliver every time in the right way, demonstrating integrity to all our stakeholders.

- Services are delivered to a high operational standard
- Reputation placed before short-term revenues
- Relentless focus on compliance with regulations and ensuring a sustainable business
- We consistently deliver on our promises to clients and to colleagues

1.3. Your Responsibilities

We rely on your personal integrity to protect our reputation.

Your responsibilities under this Code are to:

- Understand and comply with the Code
- Act fairly, honestly and with integrity when performing your duties on behalf of the Bank
- Avoid conflicts of interest
- Comply with all applicable laws and regulations
- Adhere to our policies, standards and procedures
- Observe your limits of authority when acting on behalf of the Bank
- Cooperate with any investigations, examination, litigation or inquiry related to our business
- Complete mandatory training when required
- Report any legal or regulatory proceeding that involves you personally
- Report any concerns of misconduct

Managers have a greater level of responsibility. As a manager you should also:

- Lead by example
- Promote equal opportunity and not favor or victimize any colleagues
- Help employees with ethical queries or direct them to someone who can help
- Encourage employees to report misconduct
- Protect employees from any form of retaliation if they report misconduct in good faith

We promote a culture of personal responsibility and transparency which requires you to report and discuss any actual or pending incident or risk event that you are aware of with your line manager, who may be required to further escalate the information as per the Escalation Standard.

1.4. Compliance with the Code

On joining and annually thereafter, you must acknowledge in writing or electronically that you have read and understood your obligations under the Code and the supporting policies and standards, and that you agree to comply with them.

If a situation arises where you find that you have breached this Code or any supporting policies or standards you should immediately consult your line manager and Unit Head of Compliance who will deal with the matter in a sympathetic manner and help to ensure that the breach is remedied effectively.

However, a willful breach or any failure to disclose a known breach of the Code or any supporting policies or standards could result in consequences for you and/or the Bank and may result in disciplinary action including dismissal, or in some circumstances, criminal prosecution.

1.5. Ethical Decision Making

Not every situation can be covered in the Code and our policies, standards and procedures. Here are some basic questions you can apply to help you make ethical decisions:

- Is it legal and in keeping with the spirit of the law?
- Is it consistent with our Code?
- Am I making an informed decision?
- Do I need to consult others?
- Who else could be affected by the decision?
- Could it reflect negatively on me or the Bank?
- How would it look in the media?
- Would I be embarrassed if others knew I had made this decision?
- Does it feel right?

2. Our People

2.1 Introduction

We recognize that our employees are our most valuable asset and essential for the success of our business. We aim to provide a safe working environment in which you are treated fairly and with respect.

2.2 Performance Management

We develop, support and embed a culture of high performance where relevant objectives are agreed, reviewed and assessed; where exceeding objectives is recognised; and where development is supported.

2.3 Equal Opportunities

We offer equal treatment to all job applicants and employees. We will not discriminate on the grounds of race, religion, color, nationality, ethnic or national origin, gender, marital status, disability or any other basis.

Discrimination, harassment, violence or bullying of any kind will not be tolerated.

It is each employee's responsibility to report any behavior that violates this Code. We take all reports seriously.

2.4 Fitness for Duty

You are responsible for ensuring you are fit and able to perform your duties when you report for work.

The use of alcohol or illegal drugs on our premises or during working hours is prohibited.
Showing signs of intoxication or consumption of illegal drugs may result in disciplinary action including termination of employment.

2.5 Safe Workplace

You have a personal responsibility while at work to take reasonable care of your own and others' health and safety.

In particular:

- Adhere to your local Fire, Health and Safety Procedures
- Ensure you understand the risks present in the daily work environment and take all reasonable precautions to prevent workplace accidents and injuries
- Immediately report any unsafe work conditions, serious accidents or 'near misses' to your line manager
- Know what to do in the event of an emergency
- Complete Health and Safety training as assigned by the Bank
- Participate in fire drills and building evacuation exercises

3. Our Clients and the Marketplace

3.1 Introduction

The trust of our clients and the marketplace is the cornerstone of our success.

3.2 Treating Clients Fairly

Treating clients in a fair, ethical and non-discriminatory manner, throughout the life cycle of the relationship, is an integral part of our working culture. This helps to build long-term relationships with our clients.

Always make sure:

- Communications with our clients are clear, fair and not misleading
- Only to sell approved products and services that are suitable for a client
- To handle client complaints sensitively, professionally and efficiently

Never take advantage of our clients through:

- Manipulation
- Concealment
- Abuse of privileged information
- Misrepresentation of material facts
- Any other unfair practice

3.3 Insider Trading

Insider trading undermines the integrity of the financial system by creating an unfair advantage. As an employee, you may have access to non-public material information ("Inside Information") about the Bank, our clients or other companies that we do business with. Inside Information, if it were known to the public, is likely to affect the market price of a company's securities, or affect the decision of a reasonable investor to buy or sell a company's securities.

It is a criminal offence to communicate unpublished price sensitive information to anyone who is not authorised to have it, or to act on such information.

In particular do not:

- Trade securities for your own account or any account over which you exercise control when you have Inside Information relating to those securities
- Cause anyone else to trade securities by tipping them off or passing on Inside Information relating to those securities

3.4 Confidentiality

All information that you obtain through your employment with us should be considered private and confidential and for internal use only unless clearly stated otherwise by the Information Owner in writing.

You must not disclose Bank, client or any other parties' information unless you are authorised to do so or required by law. This obligation applies even after you have left employment with the Bank.

You should use the information obtained through your employment with us only to perform your duties with the Bank. You should not use confidential information obtained while employed with previous employers.

3.5 Supplier Relationships

You must ensure that all suppliers and contractors are treated fairly and that their selection is based on price, quality of service and level of exposure to outsourcing risk. There should be no personal favoritism.

Always follow our Outsourcing Standard and your local Procurement Procedures when dealing with suppliers and contractors.

3.6 Conduct with Competitors

Any information gathered on the marketplace and our competitors must be obtained only through legal and ethical channels.

You must not engage an employee of a competitor to gain proprietary information.

3.7 Public Communication

Only designated spokespersons are permitted to issue statements on behalf of the Bank. Refer to the Media Policy for more guidance.

3.8 Political Neutrality

We are politically neutral. If you wish to participate in political activities such as campaigning or making political donations, do so in your own personal capacity and not as a representative of the Bank. Such activities should not be undertaken on our premises, using the Bank's equipment or during working hours.

4. Financial Crime

4.1 Introduction

We are committed to promoting the highest ethical and professional standards and strive to prevent the Bank from being used, intentionally or unintentionally, for financial crime.

We adhere to applicable laws, regulations and international standards. This includes the financial crime regulations issued by the Central Bank of Bahrain and by local regulators of those jurisdictions in which we operate. We also adhere to the recommendations of the Financial Action Task Force (FATF).

Financial crime includes, among others:

- Money Laundering
- Terrorist Financing
- Breach of Sanctions
- Fraud
- Bribery and Corruption
- Tax Evasion

4.2 Your Responsibilities in Combating Financial Crime

You are required to:

- Act with due care and diligence in your job role, preventing the Bank from being used as a conduit for financial crime activity

- Understand and comply with our Financial Crime Policy, Standards and Procedures
- Understand how to identify red flags indicating that a client may be seeking to engage in a relationship or transaction for other than a lawful purpose or with the proceeds of illegal activity
- Ensure sufficient customer due diligence has been conducted for new and existing client relationships, in line with the Bank's policies, standards and procedures
- Attend Financial Crime training as your job requires and achieve required pass rates
- Understand and follow applicable Sanctions restrictions and the Sanctions Policy
- Report suspicious activity immediately to your Unit MLRO
- Not "tip off" a client if you have a suspicion or if you are reporting that suspicion.

4.3 Bribery and Corruption

We take a zero-tolerance approach to bribery and corruption. This includes giving or receiving gifts, entertainment, facilitation payments or anything else of value if it is intended to obtain, or appears to give, an improper business advantage.

In many of the jurisdictions in which we operate or do business, it is a criminal offence to offer, promise, give, request, or accept a bribe, and significant penalties can be imposed if found guilty.

All gifts, entertainment and hospitality given or received with a nominal or actual value of USD 100 or above should be reported in accordance with the Anti-Bribery and Corruption Standard.

4.4 Fraud

Fraud is an unlawful act – either an act or the omission of an act – that is performed by using intentionally and personally, unfair means, and sometimes even lawful means, in order to obtain, directly or indirectly, an undue tangible or intangible advantage, or a consent, or in order to escape an obligation of any nature, for its own benefit or for the benefit of a third party.

Fraud, whether attempted or realised, is unacceptable to the Bank and its employees because it is unlawful, dishonest and threatens the Bank's reputation.

You are required to immediately report any fraud event (suspected, attempted or realised) to your Unit Head of Fraud Risk or through the available whistleblowing channels (refer to the 'Raising Concerns' section of this document).

4.5 Expenses

You are responsible for the accurate and timely reporting of expenses. All expenditures must be business related and approved in accordance with the Business Travel Standard and Business Entertainment Standard. Further, you must not use your business credit card for any purpose other than appropriate business expenses.

4.6 Charities and Non-Profit Organisations

When getting involved with a charity or non-profit organisation, remember to:

- Make sure it does not interfere with your responsibilities at the Bank
- Not solicit clients, suppliers or other employees for contributions or other participation

At times we may be asked by clients or suppliers to make a contribution to a charity or non-profit organisation. All contributions must be pre-approved by the Unit Head of Compliance to ensure they do not contravene any local laws or regulations and the Donations Policy.

5. Data Privacy and Protection

5.1. Introduction

We build trust by collecting, storing, and using personal data responsibly and ethically as per the relevant data protection laws and best practices. The protection of personal data is our responsibility and extends to all third parties that process personal data on our behalf.

5.2. Principles of Data Privacy and Protection

All employees are required to familiarise themselves with the Personal Data Protection Policy, and ensure personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to the individuals
- Processed in accordance with the purposes that it was originally identified for
- Collected only to what is necessary in relation to the purposes for which it is processed
- Correct, accurate and rectified where necessary
- Kept for no longer than is necessary for the purposes for which it is processed
- Appropriately secured and protected to preserve its Confidentiality and Integrity

5.3. Personal Data Breaches

You are required to immediately report any personal data breaches (suspected, attempted or realised) to your Local Data Protection Coordinator.

6. Protecting our Assets

6.1 Introduction

You are responsible for safeguarding the Bank's assets against theft, loss, waste or abuse. They should be used for our legitimate business only.

Our assets include:

- Office furnishings, equipment and supplies
- Software, information systems and support systems either on premises or on The Cloud
- Records and data (including backup and portable media) whether stored electronically or in paper form
- Cash and securities
- Loans and other claims on clients and third parties
- Intellectual property

- Client relationships

6.2 Information Security

Information and information systems are vital to our business and operations. Incidents involving the loss of confidentiality, integrity or availability of information can be costly and damaging to our reputation.

We may monitor, review and disclose data that you create, store, send or receive on our systems (including approved cloud-based solutions). You should not have any expectation of personal privacy when you use our systems or infrastructure.

You must adhere to our Information Security Policy. In particular, you must not:

- Use unapproved services, tools, software or cloud-based solutions to perform your job or share information with external parties or unauthorized internal personnel
- Send confidential information outside our network without using an approved encryption or security program
- Send confidential or non-public information to your personal email account
- Copy information stored on Bank assets to external media or public cloud sites
- Share business information with external parties using unapproved communication channels
- Violate software licensing agreements or intellectual property rights
- Use the Bank's computer and network resources to commit illegal activities or use them in a manner that could be embarrassing or harmful to the Bank or detrimental to its reputation or interests
- Share your username and password with anyone or have possession of anyone else's username and password
- Try to get access to or scan systems, shared folders or network areas you are not entitled to
- Make unauthorised changes on the functionality or configuration of assets under your management or control
- Leave sensitive information unattended, including your company laptop and authorized mobile devices
- Disclose or discuss sensitive matters or proprietary or confidential information in public places, including the Internet (e.g. public email, file sharing sites, social media, etc.).
- Access approved IT services, including cloud-based solutions, from unmanaged computers or portable devices.

6.3 Intellectual Property

We own all rights, title and interest in all intellectual property that you develop during your employment with us.

Intellectual property includes strategy papers, business plans, internal policies, standards and procedures, improvements, ideas, processes or work related to the Bank.

6.4 Record Keeping

You are responsible for keeping accurate and complete records in accordance with relevant laws and regulations.

7. Conflict of Interest

7.1. Introduction

It is important you avoid situations where personal interests conflict, or appear to conflict, with the interests of the Bank or our clients.

A conflict of interest exists, or may be perceived to exist, where a personal circumstance impairs professional judgment or the ability to act in the best interest of the Bank or our clients.

7.2. Avoiding Conflicts

It is difficult to identify every situation where a conflict, or perception of a conflict, may arise. You should use good judgment and seek advice from the Unit Head of Compliance if you are unsure of the proper course of action.

Typical conflicts that may arise are:

- An outside business interest
- Hiring or working with relatives, near relatives or Connected Persons (as defined in the Employment of Relatives and Connected Persons Standard)
- Dealing on your own account or using your position in the Bank to gain an unfair advantage
- Acting for the Bank in a transaction or business relationship that involves yourself, your relatives or other people or organisations where you or your relatives have a significant personal connection or financial interest

You have a responsibility to identify and disclose any conflicts or potential conflicts of interest to your Division Head, Head of HR and Head of Compliance.

7.3. Personal Finances

Conduct your own financial affairs responsibly, with integrity and in compliance with the law, to avoid situations that could reflect unfavorably on the Bank.

In general, you may not:

- Participate in personal transactions with colleagues, clients or suppliers, including investment activities (unless part of a Bank sponsored investment plan)
- Borrow from or lend money to your colleagues, clients or suppliers (except nominal amounts e.g. for lunch)

8. *Social Media Guidelines for staff*

All employees are required to familiarise themselves with the Media Policy, and display utmost caution while interacting with the media and external parties regarding all matters related to the Bank and its business.

You are required to follow the below guidelines:

- Do not share confidential information: Do not post anything confidential about the Bank or any information that is not shared by the Bank in the public domain on your personal accounts or any social media platform. You may re-share the Bank's official news and posts on your personal accounts.
- Do not speak on behalf of Bank ABC: Only official spokespeople may speak on behalf of the Bank.
- Do not open any new social media accounts on behalf of the Bank or any of its units, for internal or external audiences, without obtaining prior written consent from Group Corporate Communications.
- Treat your audiences with respect: Do not post hate, violent, threat or racist comments that you wouldn't make at the workplace.
- Think about the repercussions of what you say: Using your public voice to tarnish or malign the reputation of the Bank and that of its stakeholders may negatively impact the business of the organization you work for.
- Personal views: When posting personal views about a subject relevant to the Bank or that of its competitors, make it clear that these views are your own.
- Association: Bear in mind that as an employee of Bank ABC you are associated with the Bank. Please ensure that your social media image is consistent with how you wish to present yourself with clients and colleagues.

9. Relations with Regulators and Auditors

It is our aim to achieve excellence in compliance when meeting all relevant regulatory obligations. Maintaining a strong and positive relationship with the regulators and other government organisations is essential for ensuring the continued success of our business.

You must be completely open, candid, co-operative and prompt with regulators and external and internal auditors, keeping them fully informed about matters which should reasonably be disclosed to them.

You must:

- Refer all enquiries received from regulators to your Unit Head of Compliance
- Do not contact the regulators unless authorised to do so by your Head of Compliance[1]

[1] This does not prejudice your rights under the Group Employee Whistleblowing Policy

10. Raising Concerns

We are committed to integrity, honesty and transparency in everything we do.

You are often the first person to realise that your co-workers are participating in activities that are inappropriate or contrary to the Bank's policies, standards and procedures.

If you are aware or suspect violations to the Code of Conduct, our policies, standards and procedures, applicable laws or regulations, you are obliged to promptly report such violations using the resources described below.

We treat all reports confidentially, fairly and in a timely manner. As long as you make the report in good faith you will be protected from suffering any detriment, loss of employment or victimization.

You can raise your concerns through the Bank's Hotline, email address or mailing address as mentioned in the Group Employee Whistleblowing Policy:

Hotline: +973 1754 3710
Email: gco-wb@bank-abc.com
Mail: Group Head of Compliance, Bank ABC, P.O. Box 5698, Manama, Bahrain

If you do not receive a satisfactory response you may report your concern to the Group Chief Auditor:

Telephone: +973 1754 3350
Email: ga-wb@bank-abc.com

11. Version

Version No:	*Last Updated*
6.0	December 2020
7.0	December 2021