



Our Code of Conduct

Respect for each other, our business partners, customers, stakeholders and the law.



November 2018

A message from David LeGresley and Andrew Moor

It is our pleasure to share with you our **Code of Conduct**. As representatives of Equitable Bank, we are all responsible to uphold this commitment in tandem with our Values. Together, they stand to preserve the Bank's reputation and guide all employees in our quest to provide outstanding service as *Canada's Challenger Bank™*.

We've made our Code of Conduct easy to read so that every employee feels supported in having the confidence to ask for assistance when required. If there is any uncertainty about how the Code should be applied to a particular situation, please ensure to raise the issue with your Manager, Compliance or Human Resources who will be happy to help.



Sincerely,

David LeGresley
Chair of the Board

Andrew Moor
President & Chief Executive Officer

Table of Contents

Introduction	3
Purpose of the Code	3
Our Corporate Values.....	4
Our Role In Supporting the Code	5
Compliance with Laws and Regulations.....	5
Customer Service and Complaint Handling.....	6
Anti-Money Laundering and Anti-Terrorist Financing	6
Illegal and Anti-Competitive Sales Practices	6
Fraud and Corruption.....	6
Regulatory Inquiries & Audits	6
Other Applicable Laws.....	6
Conflicts of Interest	7
Outside Business Activities	7
Managing External Directorships.....	7
Family Members and Close Personal Relationships.....	8
Gifts and Entertainment.....	8
Protecting Bank Information and Assets.....	9
Bank Information	9
Personal Information.....	9
Accuracy of Bank Records.....	9
Protecting Bank Assets	9
Use of Information Systems	10
Insider Trading	10
Short Selling.....	10
Professional Conduct and Personal Integrity	11
Electronic Communications / Social Media.....	11
Criminal Records	12
Alcohol and Drug Use	13
Appearance.....	13
Violence & Harassment in the Workplace.....	13
Fair Treatment.....	13
Code Compliance	14
Reporting Breaches	15
Investigations	15
Policy References	16



Introduction

Equitable Bank and any of its affiliates¹ (hereinafter referred to collectively as the “Bank”) must exercise the highest degree of ethical conduct. Our colleagues, business partners, customers and the public at large have a right to expect this standard when dealing with us.

The Bank’s Code of Conduct (the “Code”) is a reflection of our guiding values and principles. As employees and directors of the Bank, we represent the Bank both at work and outside of work, and complying with the Code is an expectation. The Code serves as a central guide to connect our corporate values to a common understanding of what practices are acceptable and which are not, as we are all responsible for “doing the right thing”. Living our corporate values fosters a positive working environment, and is the key to our continued success.

Purpose of the Code

The Code outlines minimum standards of behavior expected from all employees, including contractors, and directors. It also sets out principles to guide our actions, decisions and is supported by various policies and procedures. Realistically, the Code cannot anticipate every situation that may arise. We expect reasonable judgment and common sense to be applied in all situations. If at any time you feel unsure, always ask for guidance. Never guess about compliance with the Code.

In any difficult situation ask yourself: Is this legal? Is this fair and ethical? If the situation became public, would it impact the Bank’s reputation?

¹ *Affiliates* for the purposes of the Code shall include the Bank’s parent and any of its wholly-owned subsidiaries.

Our Corporate Values

We are committed to conducting our interactions with each other, our customers, regulators, suppliers and competitors with the highest standards of integrity, honesty, fairness and professionalism, as well as treating everyone with respect, at all times and without exception. In addition, we believe that by upholding our corporate values (“Values”), the Bank will nurture a positive work environment that enhances stakeholder confidence and protects and strengthens our reputation.

Our Values guide the way we think and work to ultimately pave a better way forward as *Canada’s Challenger Bank™*. We believe that cultivating these Values helps us to deliver outstanding results in everything we do. Our Values set the standard for our daily business operations and govern our decisions and actions in all situations, irrespective of changes in strategies, type of work or job level. They apply equally to our collective activities and our conduct as individuals towards each other, customers, business partners and other stakeholders. This philosophy is central to “the way we do things around here” and critical to our continued success.

The Bank’s reputation is built and protected on these Values, which inspire our actions and decisions, and provide a benchmark for all of us.



Cherish our differences, respect each other and unite as a team by celebrating success, focusing on each other’s well-being and ensuring an inclusive workplace for all.



Through mindful personal behaviour, we consistently produce good ethical outcomes by being honest and having the courage to speak up and ask questions — even when it is hard.



Deliver outstanding service in everything we do, such as showing empathy and listening, keeping commitments with appropriate follow-through and doing all that is possible within bounds.



Support our people to make great decisions to achieve our service mission confidently and ask for clarity whenever there is uncertainty.



Embrace change to reach our goals by quickly adapting to the changing environment, challenging the status quo and using sound judgment to push forward.



Our Role in Supporting the Code

The Code applies to all Bank employees, including contractors, as well as the Bank's Board of Directors.

We all have a role to play in ensuring that the principles of the Code and our Values are promoted throughout the Bank. From our Board of Directors, who review and approve the Code, to our Chief Executive Officer (CEO) who ensures the Code is duly implemented and monitored, to our Chief Compliance Officer who works closely with Human Resources to promote awareness, adherence and compliance with the Code.

We are all expected to:

- Understand our responsibilities under the Code and its supporting policies;
- Comply with the Code and its supporting policies at all times;
- Complete any required training on the Code and its supporting policies;
- Ask for guidance when necessary; and
- Report suspected or actual breaches of the Code or its supporting policies.

If you are a people manager, you have an enhanced role and should:

- Be aware of the laws, regulatory requirements and policies related to your area of responsibility;
- Ensure all employees that report to you understand and comply with the Code; and
- Foster an environment that encourages open communication and ethical behavior.

Compliance with the Code, including its supporting policies and procedures, is mandatory. Any violations will be taken seriously and may result in disciplinary action.

Compliance with Laws and Regulations

There are a number of laws, rules, regulations and prescribed practices in place with which we must comply and which affect virtually every area of the Bank. The Bank's **Regulatory Compliance Management Policy** provides an overview of the regulatory requirements we face and how the Bank manages the laws, rules,

regulations and prescribed practices that apply to our business. Many of the key areas of law that impact our business are outlined in our policies and procedures which are referenced below and throughout the Code.

Customer Service and Complaint Handling

As part of our commitment to excellence in customer service, the Bank expects all employees to handle customer complaints promptly, fairly and transparently. Front-line employees are expected to follow our 3-step Customer Complaint Handling Procedures, and all employees are expected to report any potential compliance issues to the Bank's Ombudsman. For more information, please refer to our **Complaint Handling Policy & Corporate Procedure**.

Anti-Money Laundering and Anti-Terrorist Financing

Our business must be conducted in full compliance with all laws and regulations relating to anti-money laundering and anti-terrorist financing activities. Failure to comply may expose the Bank to the risk of legal sanctions, financial penalties and reputational damage. For more information, please consult the **Anti-Money Laundering and Anti-Terrorist Financing Policy** and related procedures or contact the Bank's Chief Anti-Money Laundering Officer.

Illegal, Anti-Competitive and Inappropriate Sales Practices

The Bank competes vigorously in the marketplace and does so ethically and legally. We do not support sales practices or agreements with other businesses that would impede free and fair competition. We do not engage in price-fixing, collusion, or coercive tied selling. We ensure our sales representations, communications and advertising to consumers are fair, clear and not misleading. In order to satisfy our commitment against coercive tied selling, we do not impose undue pressure on customers to purchase any of our products or services as a condition of approving their request for another product or service. Our sales practices reflect this commitment.

Fraud and Corruption

We comply with all laws related to combating fraud and corruption. We conduct ourselves honestly and with integrity, and we do not participate in any type of fraudulent, corrupt, or illegal transactions or activities. Examples of fraudulent and corrupt activities include, but are not limited to, bribery, commission sharing, kickbacks, theft and falsifying records.

Regulatory Inquiries & Audits

The Bank requires your full cooperation during all audits, investigations, or other lawful requests made by the Bank, regulators or government agencies. All information provided should be truthful and accurate, and documents or records should never be concealed, altered or destroyed.

Always consult your manager or the Legal Department before responding to any requests for audits, investigations or other information.

Other Applicable Laws

Always keep in mind that you are subject to all legislation and regulations related to our business. We are all personally responsible for being aware of and understanding the laws and regulatory requirements specific to our work.

Each of us must ensure we are aware of and comply with the laws, rules, regulations, policies and procedures relating to our business and our role.

All of our policies are located on our intranet at <http://sharepoint/>.



Conflicts of Interest

We must always act in the best interests of the Bank, guided by our Values, while performing our duties. Our personal interests cannot interfere, or appear to interfere, with the interests of the Bank. Conflicts could involve current or prospective employees, directors, customers, service providers, business partners or regulators.

Any perceived or potential conflict of interest is to be declared to your business unit head (or, in the case of a director, to the Chair of the Board of Directors). When in doubt about whether a conflict of interest exists, please speak with your business unit head or our General Counsel. See our **Conflict of Interest Policy** for additional guidance.

A conflict of interest includes any perceived or potential situation where the duties or position of an individual allow, or appear to allow, personal benefits or benefits to friends, relatives or businesses of that individual.

Types of situations that could cause a conflict of interest include, but are not limited to:

Outside Business Activities

Payment for services must not be accepted from any customer, business partner, service provider or competitor of the Bank and/or any directors without receiving prior approval from your business unit head. Any outside activity such as managing your own business or taking a second job must not interfere or conflict with your job performance at the Bank.

Managing External Directorships

The Bank encourages us to participate in our communities. For example, we may choose to take on directorships or similar roles at companies, organizations, clubs, associations or foundations. If so, the role must not compromise our ability to do our best work for the Bank and its customers. We must be careful to avoid actual, potential or perceived conflicts of interest and potential reputational issues. Roles and relationships must be assessed to ensure we comply with the Code and Bank policies on disclosure and approval. Generally, it is not acceptable to act as an officer or director of a customer's business.

For publicly traded, private for-profit, not-for-profit, or venture capital entities/organizations, you must obtain prior approval from the CEO. You are permitted, however, to serve on the board of private family businesses that have no relation to the Bank and its business without prior approval.



Family Members and Close Personal Relationships

It is possible for our personal relationships to have an effect on our work at the Bank. We must understand the actual or perceived effects that personal relationships can have in order to avoid situations that would reflect negatively on the Bank. This can occur in a number of situations:

- a direct supervisory relationship with a family member or close friend;
- a working relationship where we may have the ability to favourably impact compensation, work conditions or promotion prospects of a close friend or family member, including selecting or approving a service provider or vendor to the Bank;
- two employees become romantically involved.

In circumstances where family members or close friends are, or become, involved in any business activity related to the Bank, you must disclose the nature of your relationship to your business unit head or the Chief Compliance Officer and remove yourself from any related decision-making process. See our **Employee Handbook** for additional guidance.

Gifts and Entertainment

You are encouraged to consider the motive behind any gift or entertainment to ensure it is within the spirit of business courtesy and relationship management, particularly within the credit-granting functions. In addition, you must be comfortable that the gift or entertainment does not create a sense of obligation (or perception of same), influence a business decision, or could be perceived to be extravagant or excessive.

Gifts of cash or pre-loaded bankcards (e.g., Visa, MasterCard or American Express Gift Cards) are inappropriate and should never be accepted. Stored value gift cards (e.g., Cineplex, Tim Hortons, Indigo) may be accepted as long as they do not exceed \$250. You may only accept gifts with a monetary value of \$250 or less. Gifts of excessive value should be politely refused and returned with thanks and clarification of our policy (unless specifically pre-authorized by the CEO, CFO, CRO, CCO, or the SVP of Human Resources), or can be shared with your department or raffled for charity. Certain gifts such as food or candy should be shared with other employees. Occasional meals and tickets to sports or cultural events may be accepted only if they are also attended by a representative of the company or the person inviting you. Multiple gifts from the same business partner, supplier or vendor over a short period of time (within 6 months) should be avoided.

On a quarterly basis, **all** gifts and entertainment (including meals) must be **reported** to your manager using the **Gift and Entertainment Tracker**. Multiple gifts from the same donor must be listed individually. Promotional materials (e.g., pens and notepads) and gifts of nominal value (e.g., coffee purchased prior to a business meeting) need not be reported.

If in doubt, please speak with your manager, the SVP of Human Resources, or the Chief Compliance Officer.

Is this a conflict of interest? Ask yourself:

Am I following Bank policy?

Will I gain personally from my actions?

Would I act differently if a friend or relative weren't involved?



Protecting Bank Information and Assets

Bank Information

We must ensure the proper use and protection of our information. All Bank information, whether believed to be material or not, is confidential and we must treat it as such unless it is publicly disclosed. Bank information should only be disclosed internally on a “need to know” basis, and should not be disclosed externally without prior approval, unless required by law.

Further information on the handling of material and confidential information is contained in the Bank’s **Disclosure Control Policy**. The destruction of any Bank information must be handled according to the Bank’s **Records Management Policy**.

Always take precautions against accidentally disclosing confidential information - mark it appropriately, never discuss in public places, and protect your laptops, computers, iPads, iPhones and other mobile devices.

Personal Information

We protect the privacy and security of all personal information obtained while conducting our business and we limit the collection, use and disclosure of such information in accordance with applicable laws. We must ensure that

all personal information under our control, regardless of format, is protected against unauthorized access, use or disclosure. For more information, please refer to the **Privacy Policy** and related Procedures or contact the Bank’s Chief Privacy Officer.

Always report any potential or actual privacy issues to the Chief Privacy Officer immediately.

Accuracy of Bank Records

We must exercise the same ethical standards of integrity and honesty in recording our business as we do in conducting it. Individuals involved in the preparation of the Bank’s accounting, financial reports and records must accurately reflect the Bank’s business activities in accordance with our policies, procedures and regulatory requirements. We must never conceal, alter or falsify any document or record.

Protecting Bank Assets

Bank assets should only be used for legitimate business purposes and must be protected against loss, damage, theft, vandalism, sabotage, and unauthorized access, use or disclosure. Some examples of Bank assets include: Bank trademarks, corporate records, information systems and mobile devices. If you are authorized to work off-site, you must ensure that all assets used for Bank purposes are kept safe at all times.



Use of Information Systems

Our use of information systems includes our computers, telephones, mobile devices, emails, system accounts and internet access. This use should primarily be for business purposes, but occasional personal use is permitted as long as it does not interfere with your duties. You should exercise caution when using email, as statements could be misunderstood or potentially used against you or the Bank in legal proceedings. The Bank's internet connection or devices should never be used to access, transmit or download content that is inappropriate, or used to create harassing, defamatory, offensive or obscene content.

The Bank reserves the right to monitor telephone and email conversations, computer records, internet use and personal file directories to ensure compliance with the Code, as well as compliance with supporting policies and procedures. Access to social media platforms such as Facebook or Twitter is prohibited unless authorized. We are expected to use the Bank's information systems in accordance with the Bank's **Information and IT Security Handbook**.

Always remember email and internet activity is monitored.

Insider Trading

In the course of our duties, we may become aware of sensitive confidential information that others may consider important in deciding to buy or sell the securities of Equitable Group Inc. ("EGI"). We do not trade in shares of EGI, or any other company, while in possession of undisclosed material information or during a blackout period (as applicable), and we do not "tip" others. Please consult the **Insider Trading Policy** and related Procedures for further information on the Bank's practices regarding the trading of securities.

Short Selling

All employees and directors are prohibited from:

- Short selling (selling a security that you do not own) EGI securities;
- Entering into any contract that creates a short sale of an EGI security; and
- Trading in put or call options of EGI securities.

Tipping occurs when you, outside of the necessary course of business, tell another person (including your family members and friends) about material Bank information that has not been disclosed to the public. Tipping is prohibited by securities law.



Professional Conduct and Personal Integrity

We must, at all times, respect ourselves, each other and the Bank. We must act in a professional manner and with personal integrity in all our dealings with colleagues, business partners, customers, stakeholders and the public. We must live our Values in all of our interactions.

Electronic Communications/Social Media

Electronic communications and social media, whether it is business-related or personal, is subject to the guiding principles of the Code. Social media refers to websites and mobile apps that allow users to create, share and exchange content. We must ensure that we do not communicate or post anything that is confidential, proprietary, or could be harmful to the Bank's interests or reputation.

Personal use of external or internal digital communications and social media should be done responsibly as we could be considered to represent the Bank both at and outside of work. The Bank's expectations apply to all of us wherever we happen to be; whether in the workplace or not. We must be aware that any information posted online may be accessed, read or disseminated, and there can be no reasonable expectation of privacy with respect to any information posted online. We need to consider the potential impact our posts may have on the Bank's reputation, in addition to our own reputation, and be guided by our Values and the standards set out in the Code.

Some guidance when using electronic communications include the following:

- Always use appropriate and professional language;
- Consider the appropriateness of using your work email address as a point of contact for personal contacts;
- Never post material obtained from or associated with the Bank that is or could be damaging to the interests or reputation of the Bank;
- Do not use Bank logos, trademarks, or other proprietary materials without prior approval or for any purpose other than the furtherance of the Bank's legitimate business objectives in line with internal procedures;
- Do not promote specific Bank products and services as these may require certain mandatory disclosures when targeted at the public;
- Ensure that you do not compromise the confidential information of customers, employees or the Bank which includes posting to any public or external site; and
- Be alert to fraudulent activities and social engineering which look to manipulate employees into divulging confidential personal or business information or granting access to secure systems.

One of the ways the Bank communicates is through social media. As with other communications, it is important that our business and corporate social media use



is appropriate and consistent with the Bank's communication guidelines and strategy. Only authorized employees may respond to media inquiries or post content on behalf of the Bank. Except for our CEO, the SVP and Chief Digital Officer, the SVP of Marketing and Residential Sales, and the Director of Marketing Strategy and Public Relations, who are all designated to do so, we must refrain from commenting on the Bank, its business activities or competitors in any online public forum.

The Bank recognizes that employees may use a wide range of messaging technologies to directly solicit, advertise, market and promote its commercial activities to brokers and new prospects. Such messaging must adhere to prescribed consent, content and unsubscribe requirements when sending commercial electronic messages, installing computer programs or altering/re-routing data or messages. Employees must not use personal email accounts for business purposes. For more information, please refer to the **Electronic Messaging Corporate Policy**.

Always remember content posted online is public and permanent.

Criminal Records

If you are charged with, and/or found guilty of a criminal offence, you must inform Human Resources immediately. There may be employment consequences if you are charged or found guilty of an offence, including termination of employment.

The Employee Handbook and our HR policies speak to ethical business conduct. You must familiarize yourself with these and act accordingly.



Alcohol and Drug Use

While at work, we are required to be fit at all times to perform our assigned duties. We must not be impaired by the use of alcohol, cannabis or other prohibited substances. Employees and directors must ensure that they are not in possession of illegal drugs or under the influence of drugs (both legal and illegal) while on our premises, conducting business, or attending corporate events which would impair one's ability to perform assigned duties.

Appearance

As Bank representatives, our physical appearance is important. Your choice of work attire should conform to the accepted dress code standards established for our business.

Violence & Harassment in the Workplace

We are committed to respecting and protecting our employees, customers and others from violence and harassment in our workplace. Please refer to the **Violence & Harassment in the Workplace Policy** or contact Human Resources or the Chief Compliance Officer if you have any questions or concerns.

Fair Treatment

We are committed to conducting all of our affairs with fairness and equity. Treatment of employees and directors, as well as other stakeholders such as customers, business partners or service providers, should always be honest, fair and respectful regardless of race, religion, colour, country of or ethnic origin, citizenship, marital or family status, disability, gender identity, sexual orientation or age. We will not tolerate any behaviour that could be viewed as discriminatory.

We treat our co-workers, customers and others with respect and dignity at all times.



Code Compliance

You demonstrate your commitment to the Code by agreeing to comply with its guiding principles and our Values at the commencement of your employment. Annually, you will be asked to acknowledge your commitment and attest to your compliance with the Code. Your annual acknowledgement confirms that you have read, understood, and complied with the Code and its supporting policies and procedures. You will also be expected to ask questions when unclear about your responsibilities or unsure about the right thing to do, cooperate fully with internal investigations, if necessary, and report any actual or potential breach of the Code immediately.

Always feel free to speak to your manager, Human Resources or the Chief Compliance Officer if you have any questions.



Reporting Breaches

We are required to report, in good faith, any activity which is or appears to be a breach of the Code. If you believe that you have violated the Code, or suspect that someone else has, regardless of their position, you are strongly encouraged to report the breach to your manager, another manager, Human Resources, the Chief Compliance Officer or the Chair of the Audit Committee. Please refer to our **Whistleblower Policy** for more information.

The Bank will not tolerate any form of retaliation against anyone who honestly reports a concern relating to illegal or unethical conduct or a breach of any policy. At the same time, it is considered unacceptable to intentionally file a false report.

There are several channels through which you may report your concerns. Consideration should be given to the nature of the concern when choosing the appropriate channel. You can confidentially and, if desired, anonymously report an actual or potential breach to the Chief Compliance Officer or Chair of the Audit Committee. Alternatively, both the Ethics Hotline and online reporting tool are anonymous, administered by an external service provider and available seven days a week, 24 hours a day. You can also choose to report any concern to the Chief Compliance Officer or the Chair of the Audit Committee.

They can be contacted as follows:

Chief Compliance Officer

Equitable Bank
Equitable Bank Tower
30 St. Clair Avenue West, Suite 700
Toronto, Ontario M4V 3A1
(Mark the envelope as “Confidential — only to be opened by the addressee”)
Email: cco@eqbank.ca
Telephone: 416-515-3486

OR

Chair of the Audit Committee

c/o Equitable Bank
Equitable Bank Tower
30 St. Clair Avenue West, Suite 700
Toronto, Ontario M4V 3A1
(Mark the envelope as “Confidential — only to be opened by the addressee”)
Email: auditchair@eqbank.ca

OR

Ethics Hotline: **1-855-382-TALK (1-855-382-8255)**

OR

Online report: www.mycompliancereport.com/brand/equitable

Investigations

Investigations will be handled in a confidential, respectful and lawful manner. All potential breaches of the Code will be treated seriously and appropriate disciplinary action will be taken, if necessary. Action may include, but is not limited to, written warnings, demotion or re-assignment of employee, suspension with or without pay, or termination of employment.

Policy References

For more information on:	Please read:
Anti-Money Laundering and Anti-Terrorist Financing	Anti-Money Laundering & Anti-Terrorist Financing Policy and Corporate Procedures
Complaint Handling	Complaint Handling Policy and Corporate Procedure
Conflicts of Interest	Conflict of Interest Policy
Directorships and Outside Business Interests	Conflict of Interest Policy
Disclosure of Bank Information	Disclosure Control Policy and Corporate Procedures
Consent, Content and Unsubscribe Requirements for Commercial Electronic Messages	Electronic Messaging Corporate Policy
Ethical Conduct	Equitable Bank Employee Handbook
Health and Safety	Health & Safety Corporate Policy and Procedures
Insider Trading or Tipping	Insider Trading Policy and Corporate Procedures
Harassment, Discrimination and Violence in the Workplace	Violence & Harassment in the Workplace Policy
Management of Personal Information	Privacy Policy and Corporate Procedures
Overview of Regulatory Requirements	Regulatory Compliance Management Policy and Corporate Procedures
Reporting Concerns	Whistleblower Policy
Retention and Destruction of Bank records	Records Management Corporate Policy and Corporate Procedures
Use of the Internet, Email and Electronic Devices	Information and IT Security Handbook