Code of ethics and business conduct

August | 2024

A message
from the CEO

The Equifax business is built upon the trust of our stakeholders — consumers and regulators, as well as our employees, customers, partners, and investors. We all rely on trust in the products and services we deliver to enable decisions, ease transactions, and give people access to credit. Our stakeholders count on us to always do the right thing.

As we operate and grow our business, trust is central to our future. Maintaining our good reputation depends on each of us being personally responsible for our conduct and constantly on watch for the increasingly sophisticated array of threats we face.

To meet our ethics and compliance responsibilities, we must be mindful of our commitments to each other, to our customers, to our business partners, and to the communities where we work and live. Our **Code of Ethics and Business Conduct** provides guidance on our personal responsibilities and expectations of all Equifax employees, which includes complying with the laws in every market we operate in and also applying our good judgment in everything we do, each and every day.

The Code cannot answer all questions or address every situation, which is why we have established resources to provide support as different needs arise. **If you are concerned that the Code, our policies, or any laws and regulations might have been broken or will be broken, we are counting on you to speak up.** This also applies if you are uncertain about what to do in a given situation. A problem cannot be resolved unless it has first been identified, so our stakeholders all count on you to be a good steward of the Code and help with its enforcement.

I believe the quality of our people, and our commitment to ethics and compliance, will enable us to serve our stakeholders better than ever. I am convinced that working together, with the help of this Code, we will meet our goals and continue to be proud of Equifax. I am counting on you to always do the right thing... that is the only way we operate at Equifax.

Thank you for all you do.

Mark W. Begor
Chief Executive Officer

Table of contents

1 Our commitment to ethics and compliance

Protecting our reputation is the responsibility of every employee. We must always act with integrity; when we do, others will know they can trust us and have confidence that we will be honest and fair. We want to be known as a company that always honors its commitments and is a reliable business partner. When we do the right thing, we protect our reputation and that will help us to succeed even in today's complex and competitive business environment.

This Code is designed to help when you have questions about what to do in specific situations. It is a summary of how we will do business in accordance with our values, policies, and various laws and regulations.

Since Equifax operates in many countries, we need to be especially aware of different laws and customs that apply. While we respect the norms of our customers, business partners and co-workers throughout the world, all employees must at a minimum comply with local laws and the standards and principles in this Code. If you have questions or concerns please seek guidance from your local Legal team.

How to use this Code

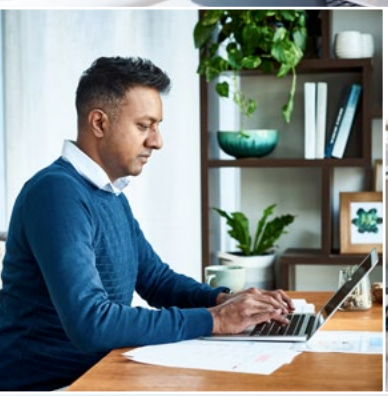
The Code is designed to serve as a resource when you need information about our policies or standards or when you are faced with a difficult ethical situation.

It's impossible to anticipate every question you may have or situation you might face, so in addition to the Code, Equifax also has other resources that can be of help. These additional resources are listed throughout the Code. As always, the Company relies on you to use good judgment and to seek help when you need it.

To whom this Code applies

This Code applies to all employees, officers and directors of Equifax. Certain business partners, such as vendors, consultants, and temporary employees, serve as an extension of Equifax. They are expected to follow the spirit of the Code, as well as any applicable contractual provisions, when working on behalf of Equifax.

Managers who supervise our business partners are responsible for ensuring that they understand our ethical standards. If an external business partner fails to comply with our ethics and compliance expectations and their related contractual obligations, it may result in a disciplinary process which may include the termination of their contract.



Asking questions

Using the Integrity Line

If you see or suspect any illegal or unethical behavior, or you have a question about what to do, talk to your supervisor and ask for help. In addition, you may submit complaints or concerns, including about Equifax information security practices, to the Equifax Integrity Line.

Sometimes, you may not be able to talk about an issue with your supervisor. If that's the case, you may contact your HR Business Partner or the Corporate Ethics Officer. You also have the option to report the activity using the following methods:

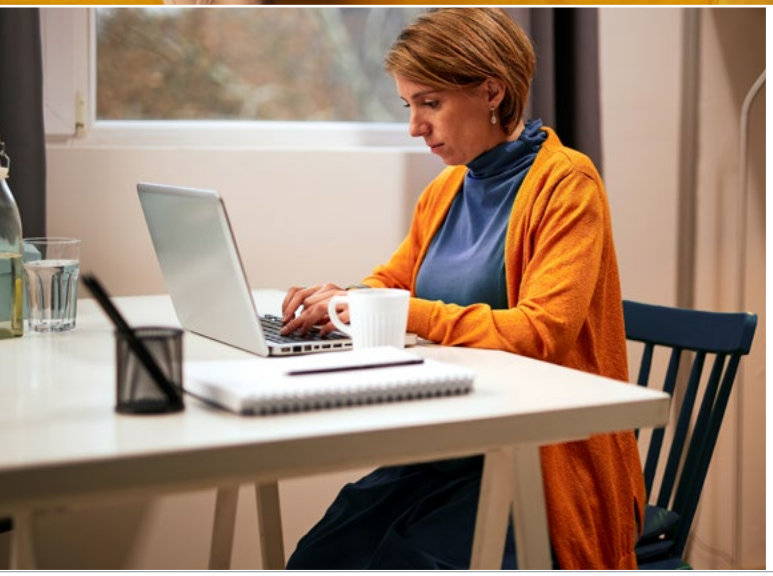
By phoning the Equifax Integrity Line

877.482.5252

For international locations, please refer to the Ethics and Integrity section on Equifax Central (the Company's intranet) for your toll-free access code when dialing.

By email to the Corporate Ethics Officer

codeofconduct.office@equifax.com



What to expect

when you use the Integrity Line

The Integrity Line is available 24 hours a day, seven days a week. Trained specialists from an independent third-party provider of corporate compliance services will answer your call, document your concerns and forward a written report to Equifax Corporate Ethics Officer for further investigation.

When you contact The Integrity Line, you may choose to remain anonymous where allowed by local law. All reports will be treated equally whether they are submitted anonymously or not.

After you make a report, you will receive an identification number so you can follow up on your concern. Following up is especially important if you have submitted a report anonymously, as we may need additional information in order to conduct an effective investigation. This identification number will also enable you to track the resolution of the case; however please note that, out of respect for privacy, the Company will not be able to inform you about individual disciplinary actions.

Equifax will use reasonable efforts to keep any report you make confidential by all individuals involved with reviewing and, if necessary, investigating it.

Equifax has an opportunity to improve every time you ask a question or raise a concern.

When you take action, speak up and report questionable conduct, you are protecting your colleagues and our reputation. Remember, an issue cannot be addressed unless it is brought to someone's attention.

Our non-retaliation policy

You can report ethical violations in confidence and without fear of retaliation. Equifax will not tolerate any retaliation against an employee who asks questions or makes good faith reports of possible violations of the Code.

Question

I suspect there may be some unethical behavior going on in my business unit involving my supervisor. I know I should report my suspicions, and I'm thinking about using the Integrity Line, but I'm concerned about retaliation.

You are required to report misconduct, and in your situation using the Integrity Line is a good option. We will investigate your suspicions and may need to talk to you to gather additional information. After you make the report, if you believe you are experiencing any retaliation, you should report it. We take claims of retaliation seriously. Reports of retaliation will be thoroughly investigated and, if they are true, retaliators will be disciplined up to and including termination.

Question

Our supervisor typically does nothing when concerns about potential misconduct are brought to her attention, and I believe she has made things difficult for co-workers who have raised issues. Now I have a problem. A co-worker is doing something that I believe to be ethically wrong. What should I do?

Take action and speak up. You are required to report misconduct. While starting with your supervisor is often the best way to efficiently address concerns, if you do not believe that it is appropriate or do not feel comfortable doing so, you should talk to another member of management, or any of the resources listed in the Code.

Employee responsibilities

Each of us must take responsibility for acting with integrity, even when this means making difficult choices. Meeting our responsibilities is what enables us to succeed and grow, today — and in the future.

- Always act in a professional, honest, and ethical manner when acting on behalf of the Company.
- Know the information in this Code, paying particular attention to the topics that pertain to your job responsibilities.
- Complete all required employee training in a timely manner and keep up-to-date on current standards and expectations.
- Report concerns about possible violations of laws, regulations, the Code or Equifax policies to your supervisor or any of the resources listed in this Code.
- Cooperate and tell the whole truth when responding to an investigation or audit and never alter or destroy records in response to an investigation or when an investigation is anticipated.

Remember: No reason, including the desire to meet business goals, should ever be an excuse for violating laws, regulations, the Code or Equifax policies.

Question

I'm a manager and I'm not clear what my obligations are if someone comes to me with an accusation — and what if it involves a senior leader?

No matter who the allegation involves, you must report it without exception. Equifax provides several avenues for reporting concerns. If for any reason you are uncomfortable making a report to a particular person, you may talk to any of the other resources listed in the Code or another member of management.

Additional responsibilities

of Equifax leadership

Equifax leaders are expected to meet the following additional responsibilities:

- Lead by example. Managers are expected to exemplify the highest standards of ethical business conduct.
- Help create a work environment that focuses on building relationships, recognizes effort, and values mutual respect and open communication.
- Be a resource for others. Communicate to employees, consultants and contract workers about how the Code applies to their daily work.
- Be proactive. Look for opportunities to discuss and address ethics and challenging situations with others.
- Create an environment where everyone feels comfortable asking questions and reporting potential violations of the Code. Respond quickly and effectively to concerns that are brought to your attention.
- Never ask or pressure anyone to do something that you would be prohibited from doing yourself.
- Ensure that Company resources are used properly and productively.
- Be aware of the limits of your authority and do not take any action that exceeds those limits. Delegate authority only where permissible and never delegate authority to any individual who you believe may engage in unlawful conduct or unethical activities.
- If you supervise third parties, ensure that they understand their ethics and compliance obligations.

Managers should not consider ethics concerns as a threat or challenge to their authority — we want an open, honest and trustful dialogue to become a natural part of daily work.

Cooperating with investigations

All employees are required to cooperate fully and truthfully with investigations. With respect to inquiries from regulators, we must never mislead any investigator and never alter or destroy documents or records in response to an investigation.

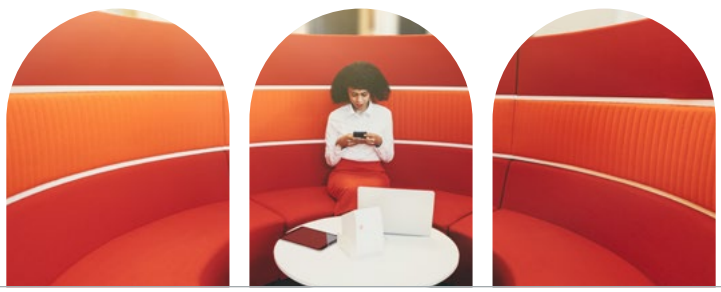
All requests for information other than what is provided on a routine basis should be reported the Equifax Corporate Ethics Officer immediately. When we are notified of an external investigation, we will take prompt action to preserve documents that may be relevant.

Investigations and inquiries

You are expected to fully cooperate and ensure that any information you provide is true, clear and complete. Prior to taking any action, consult with your HR Business Partner and/or the Legal Department.

With respect to all audits, investigations, and inquiries, you must NOT:

- Destroy, alter, or conceal any document in anticipation of or in response to a request for these documents.
- Provide or attempt to influence others to provide incomplete, false, or misleading statements to a company or government investigator.
- Conduct an investigation yourself; appropriate resources will be assigned to conduct the investigation.



Question

I'm a manager. If I observe misconduct in an area not under my supervision, am I still required to report the issue?

You are chiefly responsible for employees, contractors and third parties under your supervision, but all Equifax employees are required to report any misconduct they become aware of, and as a leader you are especially obliged to take action. The best approach is to talk first with the supervisor who oversees the area where the problem is occurring, but if this doesn't work, or isn't feasible, you should use other resources listed in the Code.

Question

I just learned that a good friend of mine has been accused of sexual harassment and that an investigation is being launched. I can't believe it's true and I think it's only fair that I give my friend an advance warning or a "heads up" so he can defend himself. Don't I have a responsibility as a friend to tell him?

Under no circumstances should you give him a "heads up." Your friend will be given the opportunity to respond to these allegations, and every effort will be made to conduct a fair and impartial investigation. An allegation of sexual harassment is a very serious matter with implications not only for the individuals involved but also for the Company. Alerting your friend could jeopardize the investigation and expose the Company to additional risk and possible costs.

Accountability and discipline

Violating relevant laws, regulations or the Code, or encouraging others to do so, exposes the Company to liability and puts our reputation at risk. If an ethics or compliance problem does occur, you are required to report it so that an effective solution can be developed. You should also understand that violations of laws or regulations may result in legal proceedings and penalties including, in some circumstances, criminal prosecution.

Waivers and exceptions

Management will regularly reassess this Code and recommend changes to the Audit Committee and the Board of Directors for approval. In extremely limited circumstances, the Company may find it appropriate to waive a provision of the Code. Any waiver of the Code for an executive officer, senior financial officer or director may only be granted by the Audit Committee or the Board of Directors, as appropriate, and will be disclosed as required by law.

Making the right decision

Making the right decision is not always easy. There will be times when you'll be under pressure or unsure of what to do. Always remember when you have a tough choice to make, you're not alone. Your colleagues and management are available to help, and you have other resources to turn to including the Code, your supervisor, and the Integrity Line.

When faced with a tough decision it may help to ask these questions:

- Is it legal?
- Is it consistent with the Code?
- Is it based on a thorough understanding of the risks involved?
- Will I be able to look myself in the mirror and be proud of the decision?
- Would I still be comfortable with the decision if it appeared in the newspaper?

If the answer to any of these questions is no, stop and speak up.

Question

My business unit sets various goals that we are asked to achieve. Sometimes I feel pressured to violate the Code and policies to achieve these goals. Is this acceptable?

No. While successful businesses set high goals and employees strive to achieve them, you should never violate the Code or Equifax policies to achieve your goals.

2 Respect and integrity in the workplace

We owe each other honesty, respect and fair treatment, and we need to always treat others as we would want to be treated. This commitment to one another is the foundation of our success. To maintain our commitment and to attract and keep talented individuals, it is vital that we continue to have a supportive, professional and respectful work environment.

Maintaining this environment not only helps Equifax succeed, it also creates the setting for each of us to thrive and to reach our full potential. What follows are some of the key areas where we must be guided by our commitment to our values and to each other.

Diversity and non-discrimination

Equifax helps bring together employees with a wide variety of backgrounds, skills and cultures. Combining such a wealth of talent and resources creates the diverse and dynamic teams that consistently drive our results.

Our colleagues, job applicants and business partners are entitled to respect and should be judged on the basis of their qualifications, demonstrated skills and achievements.

We do not tolerate discrimination based on a person's race, color, religion, ancestry, age, sex/gender (including pregnancy, childbirth, related medical conditions and sex-based stereotypes and transgender status), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law.

Make sure you:

- Treat others respectfully and professionally.
- Do not discriminate against others on the basis of any characteristic protected by law or Company policy.

Watch out for:

- Comments, jokes or materials, including emails, that others might consider offensive.
- Inappropriate bias when judging others. If you supervise others, judge them on performance. Avoid introducing unrelated considerations into your decisions. Use objective, quantifiable standards.

To learn more

Discuss any questions or concerns about diversity and equal opportunity with your supervisor or Human Resources ("HR") Business Partner.

Question

One of my co-workers sends e-mails containing jokes and derogatory comments about certain nationalities. They make me uncomfortable, but no one else has spoken up about them. What should I do?

You should notify your supervisor or HR Business Partner. Sending such jokes violates our values and our standards on diversity, harassment and discrimination. By doing nothing you are condoning discrimination and tolerating beliefs that can seriously erode the positive team environment that we have all worked to create.

Harassment-free workplace

We all have the right to work in an environment that is free from intimidation, harassment and abuse.

Verbal or physical conduct by any employee with the purpose or effect of disrupting another's work performance or creating an intimidating, offensive, abusive, or hostile work environment will not be tolerated. Equifax does not tolerate harassment of any of our employees, applicants, vendors or customers, and our policy is to maintain a working environment free from harassment.

A form of harassment is sexual harassment, which in general occurs when:

- Actions that are unwelcome are made a condition of employment or used as the basis for employment decisions such as a request for a date, a sexual favor, or other similar conduct of a sexual nature.
- An intimidating, offensive, or hostile work environment is created by unwelcome sexual advances, insulting jokes, or other offensive verbal or physical behavior of a sexual nature.

Examples of sexual harassment can include:

- Offensive sexual remarks, sexual advances, flirtations, propositions, requests for sexual favors or other verbal or nonverbal conduct of a sexual nature regardless of the gender of the individuals involved;
- Unwelcome or offensive physical conduct, including touching, regardless of the gender of the individuals involved;
- Display of offensive or derogatory pictures, drawings or photographs or other communications, including e-mail and written communications; and
- Threatening reprisals for an employee's refusal to respond favorably to sexual advances, requests for sexual favors or for reporting a violation of this Code.

At Equifax we do not tolerate:

- Threatening remarks, obscene phone calls, stalking or any other form of harassment.
- Causing physical injury to another.
- Intentionally damaging someone else's property or acting aggressively in a manner that causes someone else to fear injury.
- Threatening, intimidating or coercing others on or off the premises — at any time, for any purpose.
- Making offensive remarks, comments, jokes or slurs, or other verbal or non-verbal conduct, pertaining to or showing hostility or intimidation toward a person because of his or her race, color, religion, ancestry, age, sex/gender (including pregnancy, childbirth, related medical conditions and sex-based stereotypes and transgender status), sexual orientation, gender identity or expression, service in the Armed Forces, national origin, physical or mental disability, genetic information, citizenship status or any other status protected by law.

Question

While on a business trip, a colleague of mine repeatedly asked me out for drinks and made comments about my appearance that made me uncomfortable. I asked him to stop, but he wouldn't. We weren't in the office, and it was "after hours" so I wasn't sure what I should do. Is it harassment?

Yes, it is. This type of conduct is not tolerated, whether during working hours or in other work-related situations including business trips. You can address the situation directly by telling your colleague such actions are inappropriate and must be stopped, or you can report the issue to HR or the Corporate Ethics Officer.

Make sure you:

- Help each other by speaking out when a co-worker's conduct makes others uncomfortable.
- Never tolerate sexual harassment including requests for sexual favors or other unwelcome verbal or physical conduct of a sexual nature.
- Demonstrate professionalism. Do not visit inappropriate internet sites or display sexually explicit or offensive pictures.
- Promote a positive attitude toward policies designed to build a safe, ethical and professional workplace.
- Report all incidents of harassment and intimidation that may compromise our ability to work together and be productive. You can report such incidents to your supervisor, your HR Business Partner, the Integrity Line or the Corporate Ethics Officer. Remember that any supervisor who observes or receives a report of potential harassment must report it to Human Resources or the Corporate Ethics Officer.

Watch out for:

- Unwelcome remarks, gestures or physical contact.
- The display of sexually explicit or offensive pictures or other materials.
- Sexual or offensive jokes or comments (explicit or by innuendo) and leering.
- Verbal abuse, threats or taunting.

To learn more

Discuss any questions or concerns about our harassment policies with your supervisor or HR Business Partner.

Employee privacy

In recent years, individuals, companies and governments have grown increasingly concerned about the privacy and security of personal information. As a result, laws protecting personal information and how it may be collected, shared, and used are becoming more common.

Many of us have access to personal information related to our colleagues and others. While protecting this information may now be a legal requirement, for us at Equifax privacy has always been necessary.

Make sure you:

- Learn how Equifax classifies data, including personal information, and follow the company's requirements for protecting data both internally and when sharing externally for legitimate business purposes.
- Protect the confidentiality of personal information of current and former colleagues, as well as job applicants, business partners, customers and consumers.
- Never share colleagues' information with individuals within the company who do not have a need to know or with individuals outside the Company.
- Don't access, discuss or share confidential information unless there is a legitimate business reason to do so.
- Return or destroy personal information that is no longer required by you for business reasons in accordance with our Global Records Retention Policy.
- Immediately report to your manager any loss or inadvertent disclosure of employee information.

Watch out for:

- Unintentional exposure of confidential information in public settings such as on phone calls or while working on your laptop.
- The loss of control of confidential information. When sending personal information, both internally and externally, ensure that the disclosure is for legitimate business purpose, the data is adequately protected per the Equifax Technical Requirements, and if sending personal information to a different jurisdiction, you have authorization to do so.

To learn more

Submit any questions or concerns about employee privacy and confidential information to the Privacy and Compliance Team through AskPrivacy or access the Global Employee Privacy Statement on Equifax Central.

Safe and healthy work environment

Equifax is committed to providing a safe and healthy work environment for colleagues and visitors to our facilities. Each of us is responsible for acting in a way that protects ourselves and others.

Be proactive and speak up. The more we communicate, the better we can respond to any unsafe or unhealthy working conditions.

Situations that may pose a health, safety or environmental hazard must be reported to your HR Business Partner or your local Information Security Officer. We can only achieve our goal of a safe and healthy workplace through the active participation and support of everyone.

Make sure you:

- Observe the safety, security and health rules and practices that apply to your job.
- Be prepared to observe emergency preparedness plans if necessary.
- Always display and swipe your personal identification badge when entering and exiting secure areas, and do not allow others to enter without properly swiping their personal identification badges.
- Comply with safety and health policies and procedures.
- Maintain a neat, safe working environment by keeping work stations, aisles and other work spaces free from obstacles, wires and other potential hazards.

Watch out for:

- Unsafe practices or work conditions.
- Lax enforcement of security standards, such as facility entry procedures and password protocols.
- Threats, intimidation and violence are unacceptable and have no place at Equifax, both in our workplace or at any off-site work-related activity.
- Possession of a firearm, deadly weapon or explosives is not permitted on the company premises at any time. This applies not only to our facilities, but also to parking lots and alternative work locations maintained by the Company.

To learn more

Discuss any questions or concerns about a safe and healthy work environment with your HR Business Partner, the Global Security Office or your local Information Security Officer.

Prohibition of alcohol and drug-use

While at work or on Company business, you should never be impaired. Always be ready to carry out your work duties.

While conducting Equifax business, do not use, possess or be under the influence of illegal drugs or any substance that could interfere with a safe and effective work environment or harm the Company's reputation.

Unlawful actions that discredit the Company involving illegal drugs, controlled substances or alcohol during either working or non-working hours are grounds for disciplinary action, including termination.

Preventing workplace violence

Violence of any kind has no place at Equifax.

We won't tolerate the following:

- Intimidating, threatening or hostile behavior.
- Causing physical injury to another.
- Acts of vandalism, arson, sabotage or other criminal activities.
- The carrying of weapons on Company property.
- Offensive comments regarding violent events or behavior.
- Any other act that in management's opinion is inappropriate in the workplace.

Question

I've noticed some practices that we do in my area don't seem safe. Who can I speak to? I'm new here and don't want to be considered a troublemaker.

Discuss your concerns with your supervisor, your HR Business Partner, the Global Security Office, Local Information Security Officer, or the Corporate Ethics Officer. There may be very good reasons for the practices, but it's important to remember that raising a concern about safety does not cause trouble, it is being responsible.

Question

Are subcontractors expected to follow the same health, safety and security policies and procedures as employees?

Absolutely. Managers and supervisors are responsible for ensuring that subcontractors and vendors at work on Equifax premises understand and comply with all applicable laws, and regulations governing the particular facility, as well as with additional requirements the Company may impose.

3 Maintaining appropriate business relations

Honest and fair dealing

Equifax officers, directors and employees must deal fairly with the Company's customers, suppliers, business partners and competitors. Always tell the truth about our services and capabilities and never make promises we can't keep. Do not take unfair advantage through manipulation, concealment, abuse of privileged or confidential information, misrepresentation, fraudulent behavior, or any other unfair practice. In short, always apply the same ethical principles, of respect and teamwork, as if the partners were fellow employees.

Make sure you:

- Treat others fairly and honestly.
- Are responsive to all reasonable requests from our customers, suppliers and business partners, but never follow a request to do something that you regard as unlawful or contrary to our standards.
- Promise what you can deliver and deliver on what you promise.

Watch out for:

- Pressure from others to violate policies, rules and regulations.
- Temptations to tell people what you think they want to hear rather than the truth.

To learn more

Discuss any questions or concerns about honest and fair dealing with the Legal Department or the Corporate Ethics Officer.

Conflicts of interest

We expect Equifax officers, directors and employees to avoid any activity, investment, interest or association that interferes or appears to interfere with their independent exercise of judgment in carrying out an assigned job responsibility, or with the interests of Equifax and its shareholders as a whole. Conflicts of interest may arise in many situations. A conflict of interest occurs whenever you have a private or personal interest that may interfere with your ability to make an objective decision for Equifax. Each of us is expected to use good judgment and avoid situations that can lead to even the appearance of a conflict, which can undermine the trust others place in us and damage our reputation.

Conflicts of interest may be actual, potential or even just a matter of perception. Since these situations are not always clear-cut, you need to fully disclose them to your supervisor and HR Business Partner who will work with the Corporate Ethics Officer and the appropriate Legal Department personnel so that we can properly evaluate, monitor and manage them. Equifax officers and directors should report these matters to the Corporate Ethics Officer and the Office of Corporate Secretary.

Make sure you:

- Avoid conflict of interest situations whenever possible.
- Always make business decisions in the best interest of Equifax.
- Discuss with your supervisor and HR Business Partner (or the Corporate Ethics Officer and Office of Corporate Secretary if you are an Equifax officer or director) full details of any situation that could be perceived as a potential conflict of interest.
- Think ahead and proactively address situations that may put your interests or those of an immediate family member in potential conflict with Equifax.

Watch out for:

Situations including the following, which are common examples of potential conflicts of interest:

Corporate opportunities

If you learn about a business opportunity because of your job or position as an Equifax director, it belongs to Equifax first. This means that you should not take that opportunity for yourself unless you get approval from the Office of Corporate Secretary.

Friends and relatives

On occasion, it is possible that you may find yourself in a situation where you are working with a close friend or relative who works for a customer, supplier, competitor, etc. Since it is impossible to anticipate all situations that may create a potential conflict, you should disclose your situation to your supervisor in order to determine if any precautions need to be taken.

Outside employment

To ensure that there are no conflicts and that potential issues are addressed, you always need to disclose and discuss outside employment with your supervisor and HR Business Partner who will work with the Corporate Ethics Officer and the appropriate Legal Department personnel. If approved, you need to ensure that this outside activity does not interfere with or detract from your work. Working for a competitor, supplier, or customer may raise conflicts that will need to be resolved. Also, any approved side or personal business should not compete or do any business with Equifax.

Personal investments

You should not have a significant investment/ownership in, or obligation to, one of Equifax competitors, suppliers, customers or business partners unless you have obtained permission from the Corporate Ethics Officer. “Significant” is hard to define, but as a rule of thumb, it means that your investment should not be big enough for someone to reasonably think that you would do something at Equifax expense to help your investment. If you are unsure whether there is a conflict, you should ask for additional guidance.

Use of company property

No employee may use Company property and services for their personal benefit unless the use of that property and those services has been properly approved for general employee or public use. You must obtain prior Company approval for the use of Company-owned land, materials, equipment, etc., under any other circumstances. You must not sell, lend, give away or otherwise dispose of Company property, regardless of condition or value, without proper authorization. Additional information is included on page 26, "Protecting Our Information and Assets."

Loans and advances to directors and executive officers

Equifax is prohibited from extending or maintaining credit, or arranging for the extension or renewal of an extension of credit, in the form of a personal loan to any Equifax director or executive officer (or a family member of such person). Extensions of credit for non-executive officer employees shall be made in accordance with any other Company policy related to these matters.

Serving on a board of directors

Serving as a director on another for profit corporation, a standing committee of a similar organization, or government organizations, may create a conflict of interest. Before accepting an appointment to the board or a committee of any organization that may conflict with Equifax, you must obtain the approval of the Chief Legal Officer.

To learn more

Discuss any questions or concerns about conflicts of interest with your supervisor and HR Business Partner who will work with the Corporate Ethics Officer and the appropriate Legal Department personnel. Equifax officers and directors should discuss these matters with the Corporate Ethics Officer and the Office of Corporate Secretary.

Gifts and entertainment

In the right circumstances, a modest gift may be a thoughtful "thank you," or a meal may be an appropriate setting for a business discussion which strengthens a professional relationship. However, if not handled carefully, the exchange of gifts and entertainment can look like a conflict of interest, especially if it happens frequently or if the value is large enough that someone could reasonably think it is influencing a business decision.

When it comes to gifts and entertainment, our position is straightforward — we do not accept or provide gifts, favors, or entertainment if the intent is to influence a business decision.

Gifts and entertainment
Think before you act

Gifts and entertainment come in all different forms: fruit baskets, dinners, or tickets to sporting events, to name just a few examples. Before accepting or offering gifts or entertainment, think about the situation — does the action legitimately support Equifax's interests? Is the amount reasonable and customary? Does it conform to this Code and our policies and guidelines? And if it is a gift or entertainment that we are providing would it embarrass you or the Company if it was on the front page of the newspaper?

Make sure you:

- Only provide and accept gifts and entertainment that are reasonable complements to business relationships.
- Never accept gifts of any kind from a business partner with whom you are involved in contract negotiations.
- Exchange gifts and entertainment that foster goodwill in business relationships, but never provide or accept gifts or entertainment that obligate or appear to obligate the recipient.
- Do not request or solicit personal gifts, favors, entertainment, or services.
- Never accept gifts of cash or cash equivalents.
- Raise a concern whenever you learn of any sign or "red flag" that a colleague, third party or other agent of the Company may be engaged in any attempt to improperly influence a decision of a customer or government official.

Watch out for:

- Business partners or customers who may have gift and entertainment standards that are different than ours.
- Third parties or agents who are thought to be valuable primarily for their personal ties rather than for the services they are to perform or who request compensation out of proportion to their services.

To learn more

Discuss any questions or concerns about gifts and entertainment with the Privacy and Compliance Team, the Legal Department or the Corporate Ethics Officer.

Additional information is included in the Global Financial Crimes Policy located on the Policies site on Equifax Central.

Question

When I was traveling, I received a gift from a business partner that I believe was excessive. What should I do?

You need to let you manager know or report it to the Corporate Ethics Officer as soon as possible. Equifax may need to return the gift with a letter explaining our policy. If a gift is perishable or impractical to return, another option may be to distribute it to employees or donate it to charity, with a letter of explanation to the donor.

Question

During contract negotiations with a potential new supplier, the new supplier mentioned that they had a complimentary registration to a local business seminar. They are unable to attend and asked if I would like to go in their place. I had been thinking of attending the seminar anyway, since the subject of the seminar applies to my work. Since there's no personal gain to me, it would be good for Equifax, and it would be a shame to waste the registration, I planned on saying "yes." Would that be the right decision?

You should decline the offer. If you are involved in contract negotiations, you must never accept any gifts while the negotiation process is on-going. Accepting gifts during negotiations can give the appearance of a "quid pro quo" and is always inappropriate.

Gifts and entertainment

Government officials

Extra care needs to be taken when dealing with governments, governmental agencies, political parties, public international organizations and their officials. No gifts, entertainment, or other benefits that could be considered as intending to influence any business decision or to obtain improper advantage can be offered to public officials.

In the case of government officials, before you provide any gift, meal, travel, or entertainment or other similar type of item, be sure that it complies with our Global Financial Crimes Policy. Any request made to you or to another employee for an improper payment, or any action taken or threatened by a government official with the intent of obtaining an improper payment should be reported immediately to the Privacy and Compliance Team (ASKCompliance) or the Corporate Ethics Officer.

Supplier relations

Dealing with suppliers, contractors and customers may involve sensitive issues of law and ethics. In general, Equifax expects that all its employees shall conduct business honestly and ethically. The following guidelines supplement, but do not replace, specific criteria in the Company's purchasing or sales policies:

Treatment of others

Employees must treat all suppliers, contractors and customers fairly and honestly at all times. These parties should not be taken unfair advantage of through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair dealing.

Accepting or giving money, gifts or entertainment

No employee, personally or on behalf of the Company, should directly or indirectly request, accept, offer or give money, gifts of other than nominal value, unusual hospitality or entertainment, loans (except from lending institutions) or any other preferential treatment in dealing with any present or potential Equifax supplier, contractor, customer or competitor.

Payment to purchasing agents

No employee, personally or on behalf of the Company, should make payments to purchasing agents or other employees of any supplier, contractor or customer to either obtain or retain business, or to realize higher or lower prices for the Company. However, you may give gifts of nominal value on customary gift-giving occasions.

If you are responsible for a supplier or client relationship, you must never lead a supplier or client to believe they can inappropriately influence any procurement decisions at Equifax. Real or perceived conflicts of interest in the procurement process should be avoided.

Supplier interactions

Our suppliers and business partners are essential to our ability to do business and meet our high standards and expectations — that is why we choose them carefully and use an objective and impartial selection process.

- Avoid all conflicts of interest and favoritism in supplier relations.
- Help suppliers and business partners understand our expectations and act in a way that is consistent with our standards and applicable policies.
- Report any suspicions that a business partner may not be meeting our standards or their contractual obligations.
- Cooperate with all audits and investigations involving our business partners.

Competitive intelligence

Information about competitors is a valuable asset in today's competitive business environment. When collecting business intelligence, Equifax employees, and others who are working on our behalf, must always conduct themselves with the highest ethical standards.

We must never engage in fraud, misrepresentation or deception to obtain information. Nor should we use invasive technology to "spy" on others. We also need to be careful when accepting information from third parties, especially information that we know or could reasonably assume is confidential to a competitor. You should know and trust their sources and be sure that the knowledge they provide is not protected by trade secret laws or non-disclosure or confidentiality agreements. If you are not certain, you should err on the side of caution and contact the Legal Department prior to using or acting upon any information you receive.

While Equifax employs former employees of competitors, we recognize and respect the obligations of those employees not to use or disclose the confidential information of their former employers.

Acquiring competitive intelligence

We obtain competitive information only through legal and ethical means and never through misrepresentation, or through any behavior that could be construed as “unethical,” “espionage,” or “spying.”

Stealing proprietary information, acquiring trade secrets through bribery, possessing trade secret information that was obtained without the owner’s consent, or inducing such disclosures by past or present employees of other companies are prohibited.

Any information obtained from third parties, including information about the competition, will always be obtained and used in a strictly legal manner.

Make sure you:

- Obtain competitive information only through legal and ethical means.
- Delete or destroy competitive information that you receive without authorization.
- Never contact a competitor regarding their confidential information.
- Respect the obligations of others to keep competitive information known to them as confidential.
- Do not induce or receive competitive confidential information of other companies (such as customer pricing information).
- Make sure that third parties acting on our behalf live up to our standards.
- Do not disclose or utilize suppliers’ non-public pricing information.

Watch out for:

- Retaining papers or computer records from prior employers in violation of laws or contracts.
- Using a company’s confidential information without appropriate approvals.
- Using job interviews as a way of collecting confidential information about competitors or others.
- Asking new employees to discuss confidential information from their previous employer.
- Receiving suggestions from third parties for new products, product features, or services when the source of the original idea is not fully known.
- Obtaining information through any behavior that could be construed as “unethical,” “espionage,” “spying” or which you would not be willing to fully disclose.
- Relying, without verification, on third parties’ claims that business intelligence was obtained properly.

To learn more

Discuss any questions or concerns about collecting business intelligence with the Legal Department.

Protecting the privacy and confidential information of others

Our customers and our business partners place their trust in us. We must protect their confidential information.

Make sure you:

- Learn about the types of information which are given heightened protection by the law and Company policy (such as personally identifiable information, like social security numbers and bank account numbers) and protect them through appropriate means (such as encryption or other types of limited access).
- Never share confidential information inside or outside the Company except as authorized.
- Immediately report any loss or theft of confidential information.

Watch out for:

- Requests by business partners for information about our customers or about our business partners.
- Unintentional exposure of third-party information in public settings such as on phone calls or while working on your laptop.

To learn more

Discuss any questions or concerns about customer privacy with the Privacy and Compliance Team, the Global Security Department or your local Information Security Officer.

Additional information can be obtained in the Global Security Policies located on the Global Security Central site located on Equifax Central.

Question

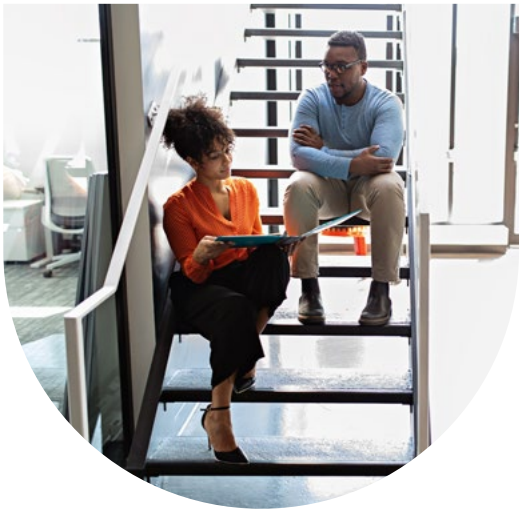
I am a manager and one of my team members who recently joined Equifax from a competitor has with her a customer list and price list of the competitor. She says she plans to use it to our advantage. Should I just ignore this and let her do it?

No. If an employee retains competitor information, it can result in legal action by the competitor. You must report this to the Legal Department for appropriate action.

Question

A customer sent me a proposal that an Equifax competitor provided. The proposal contains pricing information and product descriptions. Can I share this information with my teammates or use it to help me with the customer's business?

No. You should NOT forward the information to other Equifax employees or use the information to influence how you market or sell to the customer or for any other purpose. Instead, delete the information.



Government contracting

Equifax conducts business with governments and government-owned entities. Our policy is to comply fully with all applicable laws and regulations that apply to government contracting and transactions.

Leaders who oversee work with governments and government-owned entities must remain up-to-date on relevant regulations and should contact the Legal Department or the Corporate Ethics Officer with any questions. Special care should be taken to ensure that any third party who, while acting on behalf of Equifax provides goods or services on government projects, is aware of and abides by our high standards and their contractual obligations.

Employees working with government and government-owned entities may not participate in any private business or professional activity or have any direct or indirect financial interest that would create a conflict between their private interests and their responsibilities to Equifax. Employees who seek to participate in activities that involve outside organizations that are customers, competitors or suppliers; to serve on federal advisory committees; or to engage in other activities that could create legal or business risk must obtain prior approval from their manager, their HR Business Partner, the Legal Department and the Corporate Ethics Officer.

Employees must comply with Organizational Conflict of Interest (OCI) rules that prohibit them from serving in conflicting roles that might bias their judgment, create an unfair competitive advantage, or impair objectivity in their performance. The Legal Department must review and approve all situations that could raise OCI concerns.

Employees shall comply with all aspects of the Procurement Integrity Act, which generally prohibits employees from:

- Knowingly obtaining bid, proposal or source-selection information related to a current or future federal procurement.
- Disclosing bid, proposal or source-selection information that Equifax has received to access in the course of providing support or advice to a federal agency.
- Engaging in employment discussions with, employing or providing compensation to government procurement or contract officials in any circumstances.

Employees are responsible for seeking guidance from the Legal Department if they wish to engage with anyone who is, or has previously been, engaged with or on behalf of the government in any procurement or related action involving Equifax.

Government contracting regulations can be complex, but despite this complexity, there are a number of principles that are fundamental and apply to all employees when bidding, pricing, negotiating, and performing government contracts, including when acting as a subcontractor or when making sales to other government contractors:

- Never make or cause to be made to the government a false or fraudulent statement or a false claim for payment, whether orally or in writing. This restriction applies to bids, proposals, and requests for payment. The pricing and other terms established for a particular government contract should be followed for that contract.
- Always comply with restrictions regarding gifts or meals for government employees. Government employees are subject to strict rules which require them to pay for their own expenses with limited exceptions.
- Always use legitimate methods to obtain a contract. Never seek or receive information that the Company is not authorized to possess, including, but not limited to, confidential or proprietary data, pricing information of other competitors for government contracts, and non-public government documents relating to bidding or source selection.
- Always comply with federal and state conflict of interest restrictions which restrict the ability of former government officials or employees to represent, aid, or advise the Company on governmental matters in which the former official or employee had some governmental responsibility or involvement. No former government official or employee may be hired or retained by the Company in any capacity without the prior review and approval of the Legal Department.

4 Protecting our information and assets

Protecting Equifax assets

We are entrusted with Company assets and are personally responsible for protecting them and using them with care. Company assets include funds, facilities, equipment, information systems, intellectual property and confidential information.

Make sure you:

- Personal use of Company assets is discouraged, should be kept to a minimum and should have no adverse effect on productivity and the work environment.
- Do not use Equifax equipment or information systems to create, store or send content that others might find offensive.
- Do not share passwords or allow other people, including friends and family, to use Equifax resources.
- Avoid any use of Company assets that might cause loss to the Company or damage to the assets.
- Respect the copyrights, trademarks and license agreements of others when dealing with printed or electronic materials, software or other media content.
- If you suspect any fraud or theft of company assets, immediately tell your supervisor or someone from Human Resources, the Corporate Ethics Officer, or the Audit Committee of the Board of Directors.
- Only use software that has been properly licensed. The copying or use of unlicensed or "pirated" software on Company computers or other equipment to conduct company business is strictly prohibited. If you have any questions about whether or not a particular use of software is licensed, contact the IT Asset Management Group or the Corporate Ethics Officer.
- You should handle carefully any documents containing confidential information during working hours, and properly secure them at the end of the business day. You should pay particular attention to the security of data stored on your computer systems. You must maintain the secrecy of all computer systems, and secure any equipment when not in use.

Watch out for:

- Company property that is not secured when not in use.
- Requests to borrow or use Equifax equipment without approval.
- Unknown individuals without proper credentials in our facilities.
- Excessive use of Equifax resources for personal purposes.
- Lax enforcement of electronic access control cards.
- Sharing passwords.

To learn more

Discuss any questions, concerns about protecting Equifax assets with the Global Security Office or your local Information Security Officer.

Additional information can be obtained in the Global Security Policies located on the Global Security Central site located on Equifax Central.

Confidential information and intellectual property

One of our most valuable assets is information. Each of us must be vigilant and protect confidential information. This means keeping it secure, limiting access to those who have a need to know in order to do their job, and avoiding discussion of confidential information in public areas.

Confidential information includes all non-public information that might be of use to competitors, or harmful to the Company or its customers, if disclosed. The obligation to preserve confidential information continues even after employment ends.

Make sure you:

- Use and disclose confidential information only for legitimate business purposes.
- Properly label confidential information to indicate how it should be handled, distributed and destroyed.
- Protect intellectual property and confidential information by sharing it only with authorized parties.
- Only store or communicate Company information using Equifax information systems.
- Never discuss confidential information when others might be able to overhear what is being said — for example on planes or elevators and when using mobile phones.
- Do not send confidential information to unattended fax machines or printers.

Watch out for:

- Unintentional exposure of confidential information in public settings, including industry conferences, public conversations or phone calls, or public use of laptops.
- The loss of control of confidential information. When sending personal information to third parties, make sure that the transmissions are for legitimate business reasons and that they comply with local law.
- Communications about ongoing or anticipated litigation without guidance from the Legal Department.

To learn more

Discuss any questions or concerns about confidential information with the Global Security Office or your local Information Security Officer.

Additional information can be obtained in the Global Security Policies located on the Global Security Central site located on Equifax Central.

Confidential information includes, but is not limited to:

- Operational data and reports
- Customer and supplier lists
- Personnel information and records
- Pricing information
- Company financial information that has not been released to the public
- Software programs developed by employees or specifically for the Company
- Business and strategic plans
- Intellectual property, “know how” and inventions
- Technology, operations, research and technical data
- Third-party information and records (e.g. belonging to vendors, suppliers, etc.) given to us in confidence
- Privileged communications with the Legal Department

Intellectual property

Equifax intellectual property rights are extremely valuable to the Company. They are also extremely "fragile," because they can be compromised or even forfeited if we do not vigilantly protect them. In order to protect the Company's intellectual property, all Equifax employees and contractors should use best efforts to:

- Recognize and identify the Company's actual or potential intellectual property assets;
- Notify the appropriate Equifax personnel (either a senior technology officer, the Legal Department or the Corporate Ethics Officer) of the existence and development of intellectual property assets and promptly disclose to company management any inventions or other intellectual property that you create while you are employed by Equifax;
- Assist in securing the Company's ownership of intellectual property assets and sharing them with authorized parties;
- Assist, where appropriate, in registering, patenting, or otherwise legally protecting intellectual property assets;
- Otherwise properly label confidential information including intellectual property to indicate how it should be handled, distributed and destroyed;
- Use the intellectual property assets properly, including in licensing and other transactions;
- Prevent any infringement or misuse of the Company's intellectual property;
- Notify the appropriate Equifax personnel (your supervisor, the Legal Department or the Corporate Ethics Officer) of any potential infringement or misuse of the Company's intellectual property, so that we may take appropriate action; and
- Have outside vendors, contractors, licensees, joint venture partners and employees sign the appropriate Equifax documents acknowledging Equifax intellectual property ownership. (Consult with the Legal Department regarding appropriate Equifax documents.)

Some examples of our intellectual property assets are:

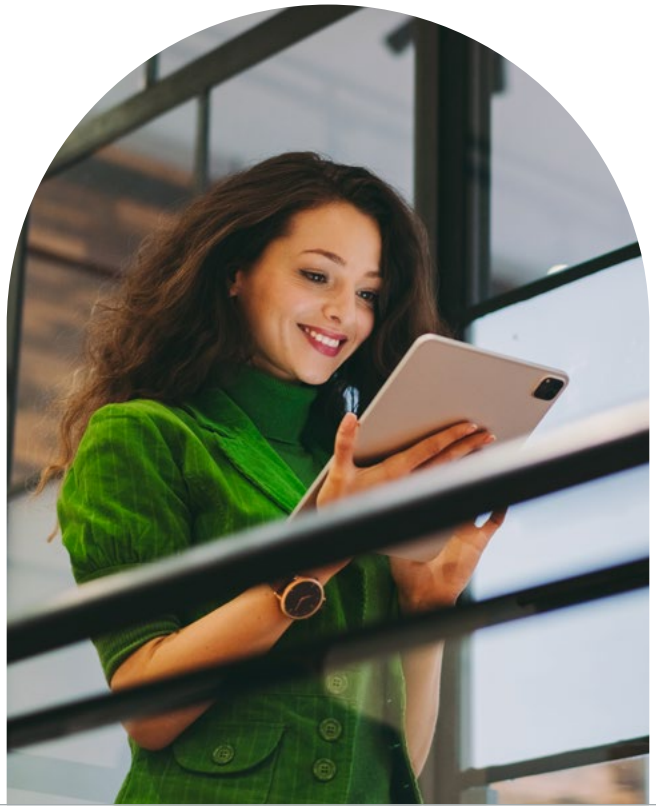
- Business and marketing plans
- Company initiatives (existing, planned, proposed or developing)
- Customer lists
- Trade secrets and discoveries
- Methods, know-how and techniques
- Innovations and designs
- Systems, software and technology
- Patents, trademarks and copyrights

Creating and managing our business records

Business partners, government officials and the public need to be able to rely on the accuracy and completeness of our disclosures and business records. Accurate information is also essential within the Company so that we can make good decisions.

Our books and records must be clear, complete and in compliance with accepted accounting rules and controls. Employees with a role in financial or operational recording or reporting have a special responsibility in this area, but all of us contribute to the process of recording business results and maintaining records. Each of us is responsible for helping to ensure the information we record is accurate and complete and maintained in a manner that is consistent with our system of internal controls.

If you suspect any irregularity relating to the integrity of our records, you need to report it immediately to your supervisor, the Legal Department or the Corporate Ethics Officer.



Managing our records

Equifax has a Global Records Retention Policy and Record Retention Standard to ensure records are maintained, stored and destroyed, when appropriate, in accordance with our business needs and in compliance with applicable regulations. From time to time, the Company establishes retention or destruction standards for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management. We expect all employees to fully comply with the Global Records Retention Policy and Records Retention Standard.

Each of us is responsible for information and records under our control. We must be familiar with the recordkeeping procedures that apply to our jobs, and we are accountable for the accuracy and truthfulness of the records we produce. It is also our responsibility to keep our records organized so that they can be located and retrieved when needed.

Documents should only be destroyed in accordance with our Global Records Retention Policy, and never in response to or in anticipation of an investigation or audit. Contact the Privacy and Compliance Team or the Legal Department if there is any doubt about the appropriateness of record destruction.

Litigation exception

If you believe, or the Company informs you, that Company records in any form are relevant to litigation or potential litigation (i.e., a dispute or regulatory matter that could result in litigation), then you must preserve those records until the Legal Department determines the records are no longer needed. This exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that this exception may apply, or have any question regarding the possible applicability of that exception, please contact your supervisor, the Legal Department or the Corporate Ethics Officer.

Make sure you:

- Create accounting and business records that accurately reflect the truth of the underlying event or transaction.
- Record transactions as prescribed by our system of internal controls.
- Write carefully, professionally, and clearly in all your business communications, including emails, chat messages, and text messages. Write with the understanding that someday they may become public documents, especially when discussing confidential or sensitive topics. Be mindful of the rules and policies regarding attorney-client privilege and confidentiality.
- Sign only documents — including contracts — you have reviewed, are authorized to sign, and believe are accurate and truthful.
- Do not record false sales or record them early, understate or overstate known liabilities and assets, or defer recording items that should be expensed.
- Retain, protect and dispose of records according to our Global Records Retention Policy. Records subject to legal hold notices, document preservation requests or regulatory requirements may be subject to additional protections.
- If your job involves financial or operational recording or reporting, know all Equifax policies that apply.
- Strictly follow the instructions within any applicable Legal Holds.

Watch out for:

- Requests to retain records due to a legal hold.
- The premature or overdue destruction of records.
- Unintentional retention of records that should be destroyed.
- False claims on an expense report or time sheet.
- Financial entries that are not clear and complete or which hide or disguise the true nature of any transaction.
- Undisclosed or unrecorded funds, assets or liabilities.
- Interference with the auditing of Equifax financial records.

To learn more

Discuss any questions or concerns about our records management and disclosure processes, legal holds or attorney-client privilege with the Legal Department or the Corporate Ethics Officer.

Additional information can be obtained in the Global Records Retention Policy or the Corporate Accounting Policies located on the Policies site on Equifax Central.

Question

At the end of the last quarterly reporting period, my supervisor asked me to record additional expenses even though I had not yet received the invoices from the supplier and the work has not yet started. I agreed to do it, mostly because I didn't think it really made a difference since we were all sure that the work would be completed in the next quarter. Now I wonder if I did the right thing.

No, you did not. Costs must be recorded in the period in which they are incurred. The work was not started and the costs were not incurred by the date you recorded the transaction. It was therefore a misrepresentation and, depending on the circumstances, could amount to fraud.

Communicating with the public

Equifax needs a consistent voice when making disclosures or providing information. It is important that only authorized persons speak on behalf of the Company. We must maintain the highest standards of integrity, objectivity and transparency. We are committed to honest, professional and legally compliant communications to colleagues, business partners, and the public. Accordingly, except as otherwise designated by the Company's Chief Executive Officer, the Corporate Communications Department (Corporate Communications) is the sole contact for media seeking information from Equifax. Any requests from the media must be referred to Corporate Communications. They will deal directly with the media and make appropriate arrangements. Corporate Communications must approve any article, press release, or any other public communication involving the Company prior to publication.

Make sure you:

- Refer inquiries about our activities, sales or financial results, or strategic plans to Corporate Communications.
- Always get prior approval from Corporate Communications before making public speeches, writing articles for professional journals or making other public communications when you are identified as an employee of the Company.
- Obtain approval from Corporate Communications before distributing any communication intended for a broad employee audience. Communications intended for inter-Company distribution require pre-approval as well.
- Never give the impression that you are speaking on behalf of the Company in any personal communication, including social media user forums, blogs, chat rooms and bulletin boards.
- Never speak for the Company in your personal communications, including in emails, blogs, message boards and social media platforms.
- Do not use your Company title or affiliation outside work for Equifax — such as in charitable or community work — without making clear the fact that the use is for identification only and that you are not representing the Company.

To learn more

Discuss any questions or concerns about communicating with the public with Corporate Communications.

Additional information can be obtained in the Global External Communications Policies and Guidelines and the Corporate Disclosure Policy located at Equifax Central.

Using social media

We need to be careful when engaging in communications that might be published online. If you participate in online forums, blogs, newsgroups, chat rooms, or bulletin boards, think carefully before you hit the "send" button.

When using social media:

- Never publish or comment on confidential and non-public Company information such as the Company's current or future business performance or business plans.
- Be fair and courteous, and never post content that may be viewed as malicious, obscene, harassing, defamatory or discriminatory.
- If you read a comment about Equifax that you believe is wrong, do not respond. Instead, contact Corporate Communications so that appropriate steps can be taken.

To learn more

Additional information can be obtained in the Social Media Policy located in the Policies section of Equifax Central.

Use of Artificial Intelligence (AI)

Equifax has been using Artificial Intelligence (AI) Systems over the past decade and recognizes that AI can help increase productivity and innovation. Equifax is committed to Responsible AI, using AI Systems in a transparent, trustworthy, fair, explainable, and secure manner while providing benefits to consumers, customers, and our technical and business operations. Employees are required to use AI Systems in accordance with this Code and the End User Security Policy.

Equifax has established an AI Governance Program to help ensure it is meeting its obligations for using AI Systems appropriately, responsibly, and in compliance with applicable laws and regulations. Specifically, the AI Governance Program is designed to set the strategic direction, provide global oversight of the use of AI Systems, and define the principles and practices that comprise Responsible AI at Equifax.

Equifax has approved limited AI Systems for use across the Company, published by TechRadar, and has defined three (3) categories of use cases for AI Systems:

- **Innovation:** The use of AI Systems and techniques to develop new products or services, or enhance existing products or services, for use by Equifax customers.
- **Internal Development:** The use of AI Systems to support new application development and deployment.
- **Operational Improvement:** The use of AI Systems to improve operational processes to drive efficiencies.

Any additional categories of use cases must be approved through the Steering Committee of the AI Governance Program.

To learn more

The Global AI Policy and AI Governance Program Charter may be found on the Privacy and Compliance Team Site on Equifax Central. Additional resources are available on the EFX.AI Resource Center on Equifax Central.

5 Following the letter and spirit of the law

Political activities

You have the right to voluntarily participate in the political process including making personal political contributions. However, you must always make it clear that your personal views and actions are not those of the Company.

In addition, you must never use Equifax funds, assets or resources to support any political candidate or party unless specifically permitted by law and authorized in accordance with the Company's Political Engagement Policy and Political Activity guidelines. Federal law and Company policy also states that the Company will not reimburse anyone for personal political contributions.

Every employee and director of the Company is subject to and has a personal responsibility to review and understand the Company's Political Engagement Policy and Political Activity Guidelines.

Make sure you:

- Are clear that your personal political views and activities are not viewed as those of the Company.
- Do not use Equifax resources or facilities to support your personal political activities.
- Inform and coordinate with the Legal Department prior to interacting with or discussing policy matters of interest to the Company with government officials or regulators.

Watch out for:

Lobbying

Interactions with government officials or regulators that could be seen as lobbying must be discussed in advance and coordinated with the Legal Department.

Pressure

Never apply direct or indirect pressure on another employee, customer or business partner to contribute to, support, or oppose any political candidate or party.

Improper influence

Avoid even the appearance that you are making political or charitable contributions in order to gain favor or in an attempt to exert improper influence.

Conflicts of interest

Holding or campaigning for political office must not create, or appear to create, a conflict of interest with your duties.

To learn more

Discuss any questions, concerns about political contributions or political activities, with the Legal Department.

Insider trading

Insider trading and "tipping" prohibited

No Equifax employee, officer, director or other "insider" may purchase or sell Equifax securities while in possession of material, nonpublic information relating to Equifax ("insider trading"). In addition, no Equifax employee, officer, director or other insider may disclose material, nonpublic information about Equifax, or any other company with which Equifax deals, to others ("tipping"), unless authorized to do so.

Additional trading restrictions may apply

In addition to the general prohibitions against insider trading and tipping, certain insiders with regular access to material, nonpublic information may only trade in Equifax securities during specified trading windows and/or pursuant to pre-clearance and reporting requirements. In addition, Equifax officers and Section 1b reporting persons may only purchase or sell Equifax securities pursuant to a Rule 1065-1 trading plan that has been approved by the Office of Corporate Secretary. You will be notified by the Office of Corporate Secretary if you are subject to these additional restrictions.

Covered insiders

The concept of "insider" is broad. It includes all Equifax employees, officers and directors, as well as their family members, friends and other related parties. It also includes other persons (including consultants, accountants, legal counsel and other advisors) who are not employed by Equifax but who have access to material, nonpublic information about the Company.

Insider trading is a serious crime

The penalties for insider trading or tipping are severe, both for the individuals involved in the unlawful conduct and their employers. Where a violation occurs, a person can be subject to substantial penalties, including criminal liability, civil liability and disciplinary action (up to termination of employment).

Material, nonpublic information

Information is considered "material" if:

- a reasonable investor would consider the information important in making a decision of whether to buy, hold or sell a security;
- a reasonable investor would view the information as significantly altering the total mix of information in the marketplace about the company that issued the security; or
- the information could reasonably be expected to have a substantial effect (positive or negative) on the price of the security.

Some examples of information about a company that might be material are:

- Financial or operating results
- Discussions regarding a merger, acquisition, disposition or joint venture
- Changes in top management
- An expansion or cutback of operations
- The introduction or development of a new product or service
- A significant legislative or regulatory development
- A cybersecurity incident, security breach or other material disruption of the Company's information technology infrastructure

Information is "nonpublic" until it has been "publicly disclosed," meaning that it:

- is published in such a way as to provide broad, non-exclusionary distribution of the information to the public; and
- has been in the public domain for a sufficient period of time to be absorbed by the market and reflected in the price of the related securities.

Examples of public disclosure include the issuance of a press release or the filing of a report with the Securities and Exchange Commission. Information is generally considered to be nonpublic until the expiration of a period of one full trading day after the information is released to the general public.

Make sure you:

- Do not share material, nonpublic information with anyone, including other Equifax employees, unless you are authorized to do so.
- Do not buy or sell, or advise anyone else to buy or sell, the securities of Equifax (or such other company) if you are in possession of material, nonpublic information regarding Equifax (or material, nonpublic information regarding any other publicly-traded company that you have obtained as a result of your employment with Equifax), until that information has been publicly disclosed.

Watch out for:

Requests by friends or family for information about Equifax or companies that we do business with or have confidential information about. Giving this information to anyone else who might make an investment decision based on your inside information is considered "tipping" and is against the law, regardless of whether you benefit from the outcome of their trading.

To learn more

See the Company's Insider Trading Policy and Corporate Disclosure Policy, both of which are available on Equifax Central.

Discuss any questions or concerns about insider trading with the Chief Legal Officer or the Office of Corporate Secretary.

Question

I'm not sure what kind of information is covered by the term "material information." What does it include?

"Material information" includes any information that a reasonable investor would consider important when deciding whether to buy, sell or hold a security. There is no bright-line standard for assessing materiality. Rather, materiality is based on an assessment of all of the facts and circumstances, and is often evaluated by enforcement authorities with the benefit of hindsight. If you're in doubt about whether certain information is material or has been released to the public, don't trade until you have consulted with the Chief Legal Officer or the Office of Corporate Secretary.

Anti-trust and fair competition

We believe in free and open competition and never engage in improper practices that may limit competition. We never look to gain competitive advantages through unethical or illegal business practices, but rather through superior performance.

We do not enter into agreements with competitors to engage in any anti-competitive behavior, including setting prices or dividing up customers, suppliers or markets.

Anti-trust laws are complex and compliance requirements can vary depending on the circumstance, but in general, the following activities are red flags and should be avoided and reported to the Legal Department:

Collusion

When companies secretly communicate or agree on how they will compete. This could include agreements or exchanges of information on pricing, terms, wages, or allocations of markets. This may also include agreements not to solicit or hire a competitor's employee.

Bid-rigging

When competitors or service providers manipulate bidding so that fair competition is limited. This may include comparing bids, agreeing to refrain from bidding or knowingly submitting noncompetitive bids.

Predatory pricing

When a company with market power sells a product or service below cost so as to eliminate or harm a competitor, intending to recover the loss of revenue later by raising prices after the competitor has been eliminated or harmed.

- Do not discuss current or future market prices, price adjustments or discounts with competitors.
- Do not discuss profit levels sought or attained with competitors.
- Do not make any agreements concerning treatment of a customer, potential customer, supplier or potential supplier.

Watch out for:

- Temptations to engage in informal conversations with competitors about competitively sensitive information. A conversation may be a breach of competition law whether it is formal or informal.
- When representing the Company in trade association activities, employees must be careful not to share pricing or other non-public competitive information, or engage in any other activity that could reasonably be construed as price fixing or in restraint of trade.
- Conversations with competitors that could be perceived as limiting competition. If such a conversation begins, leave the meeting immediately and report it to the Legal Department or the Corporate Ethics Officer.

To learn more

Discuss any questions or concerns about anti-trust and anti-competitive business practices with the Legal Department or the Corporate Ethics Officer.

Question

I received sensitive pricing information from one of our competitors. What should I do?

You should contact the Legal Department and or the Corporate Ethics Officer without delay and before any further action is taken. It is important that from the moment we receive such information we demonstrate respect for antitrust laws and we make clear that we expect others to do the same. This requires appropriate action that can only be decided on a case-to-case basis and may include sending a letter to the competitor.

Anti-corruption and bribery

Equifax has a global commitment to integrity. We do not pay bribes or kickbacks, at any time for any reason. As defined in the Global Financial Crimes Policy, Equifax strictly prohibits the offering, giving, solicitation or acceptance of any bribe, or corrupt inducement whether in cash or any other form. You may not give, offer or promise (directly or through others) anything of value to anyone, including government officials, clients, suppliers or other business partners, if it is intended or appears intended to obtain some improper business advantage. This prohibition applies equally to agents and representatives of Equifax acting on the Company's behalf.

It is especially important that we carefully monitor third parties acting on our behalf. We must always be sure to perform due diligence and know our business partners, consultants, agents, and all those through whom we conduct our business. We must know who they are and what they are doing on our behalf and they must understand that they are required to operate in strict compliance with our standards and to maintain accurate records of all transactions.

Question

I work with a foreign agent in connection with obtaining certain approvals in the United Kingdom. I suspect that some of the money we pay him goes toward making payments or bribes to government officials. What should I do?

This matter should be reported to the Legal Department or the Corporate Ethics Officer for investigation. If there is bribery and we fail to act, both you and Equifax could be liable. While investigating these kinds of matters can be culturally difficult in some countries, any agent doing business with Equifax should understand the necessity of these measures. It is important and appropriate to remind Equifax agents of this policy.

If you are ever offered or asked for a bribe

If you are offered or asked for a bribe, no matter how small, you must refuse it and clearly state our policy of never engaging in bribery or corruption. You should then immediately report the incident to the Corporate Ethics Officer.

Giving or accepting any form of bribe is serious misconduct and will be treated as a disciplinary matter.

Make sure you:

- Never give anything of value inconsistent with local laws and regulations to any governmental officials. If you are not sure what the local laws are, the safest course of action is to not give anything of value.
- Do not engage an agent, consultant, or advisor who may have dealings with foreign governments or political parties on behalf of Equifax; or make or allow to be made any payment arrangements where a person performing services or selling goods in one country requests that payments be made in another country.
- Understand the standards set forth under applicable anti-bribery and anti-corruption laws which apply to your role at Equifax.
- Accurately and completely record all payments to third parties.
- Make no “facilitating payments” to a public official.

Watch out for:

- Apparent violations of anti-bribery and anti-corruption laws by our business partners.
- Agents who do not wish to have all terms of their engagement with Equifax clearly documented in writing.

To learn more

Discuss any questions or concerns about anti-corruption and bribery with the Privacy and Compliance Team, the Legal Department or the Corporate Ethics Officer.

Additional information can be attained in the Global Financial Crimes Policy located on Equifax Central.

6 Conclusion

Protecting our reputation is the responsibility of every employee. We must always act with integrity; when we do, others will know they can trust us and have confidence that we will be honest and fair. Every day we demonstrate our commitment to this Code through our decisions and actions. Our reputation depends on our ability to do the right thing by always honoring our commitments.

This Code is designed to help when you have questions about what to do in specific situations. It is a summary of how we will do business in accordance with our values, policies, and various laws and regulations. If you have questions about the Code or you are not sure what to do in any situation, you can contact the Corporate Ethics Officer for guidance.

It all starts with *you*