Global Code of Conduct

Living our core values

Table of contents

A message from our **Chair, President, and CEO**

People want to work for—and do business with—companies they trust. This is true in any industry, but it's especially critical in ours. That trust is earned over time—often years or decades—and reinforced through everyday actions, including how we work with one another and the decisions we make on behalf of our customers. Each of us plays an important role in protecting that trust. The way we support, respect, and challenge one another internally directly influences how we serve our customers and deliver on our commitments.

Our core values, including ***Do what's right***, guide how we serve our customers and how we work with one another at Principal. Our Global Code of Conduct (Code) turns those values into practical guidance and provides clear expectations for how we act, make decisions, and conduct business every day. I ask each of you to take time to read the Code carefully and apply it consistently in your work.

While the Code is comprehensive, it can't address every situation. Use good judgment and ask for additional guidance when needed (resources and contacts are listed within the Code). Remember, if you're concerned that a decision or action is a possible violation of the Code, it's your responsibility to speak up. Raising concerns is essential to maintaining integrity across our organization, at every level, and helps us identify risks early so they can be mitigated and the culture of ethics we all value is maintained.

Our commitment to integrity has been built over 146 years, and we are the stewards of that legacy. Thank you for conducting business in a way that instills our values and strengthens our culture.

Deanna

Deanna Strable
Chair, President, and CEO

A message from our **Enterprise Chief Ethics and Compliance Officer**

Thanks, Deanna, for role modeling the ethical behavior that defines who we are at Principal. To my fellow employees, as your Enterprise Chief Ethics and Compliance Officer, I want to reinforce the importance of being familiar with, understanding, and following our Global Code of Conduct (Code). While the Code advocates an ethical culture, conveys the core values we wish to foster in leaders and employees, and defines desired behavior, being ethical is more than just words on paper. It transcends policies and procedures. It's about doing what's right in daily decisions. As employees of Principal, we have an obligation to uphold promises and commitments reflected in our Code to each other, our customers, and other key stakeholders.

Customers want to work with a company they can trust, and employees are proud to work for a company known for its ethical culture. As employees, we are all stewards of maintaining the ethical culture that is core to Principal. Thank you for all you do each day to ensure we continue to do what's right and conduct our business with integrity.

Noreen

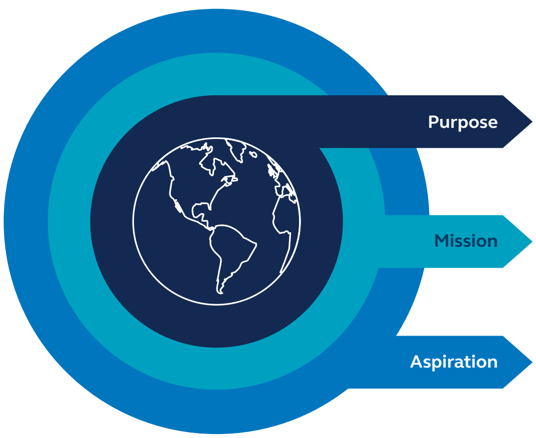
Noreen Fierro
Sr. Vice President and Enterprise Chief Ethics and Compliance Officer

Our purpose, mission, and core values

The Code explains how we conduct business at Principal® – every day, wherever we do business – to continually earn and maintain our reputation of integrity. It applies to all wholly and majority-owned entities of Principal Financial Group® (Principal) throughout the world.

The Code has been approved by our senior leadership and the Board of Directors. We disclose our Code and any additions or changes on our website (www.principal.com).

Our purpose, mission, and aspiration



Foster a world where financial security is accessible to all

Help more people save enough, protect enough, and have enough

Inspire trust by exceeding customer and partner expectations, leading the way to financial confidence

Core values

Our core values are the ideals we won't compromise in pursuit of our purpose, mission, and aspiration; they help guide our day-to-day actions. Core values are the foundation of our culture.

The core values that guide the role you play are highlighted at the bottom of the first page of each section.

Start with the customer

We solve for the customer—every day and with every decision.

Do what's right

Integrity is nonnegotiable. It guides everything we do.

Own what's next

We continuously learn and advance ourselves in pursuit of tomorrow.

Invest for our future

We make smart decisions with our resources to ensure our customers' future success and ours.

Using this code

What's expected of me?

Follow our Code
Every director and employee of Principal, regardless of function, position, or location, is accountable for following this Code. We expect anyone who represents us (such as minority-owned joint ventures, salespersons, suppliers, and consultants) to follow standards that are consistent with this Code.

Comply with laws
Our business is highly regulated and is conducted in many locations, so we are subject to multiple, and sometimes differing, laws and regulations. We're committed to conducting business in full compliance with applicable laws and regulations of the countries and communities in which we do business. We must each be familiar with, and act in compliance with those that affect our work. Laws are often complex. Please consult with the Law Department or your local legal contact if you have questions or concerns. But your role doesn't stop with simply complying with laws and regulations.

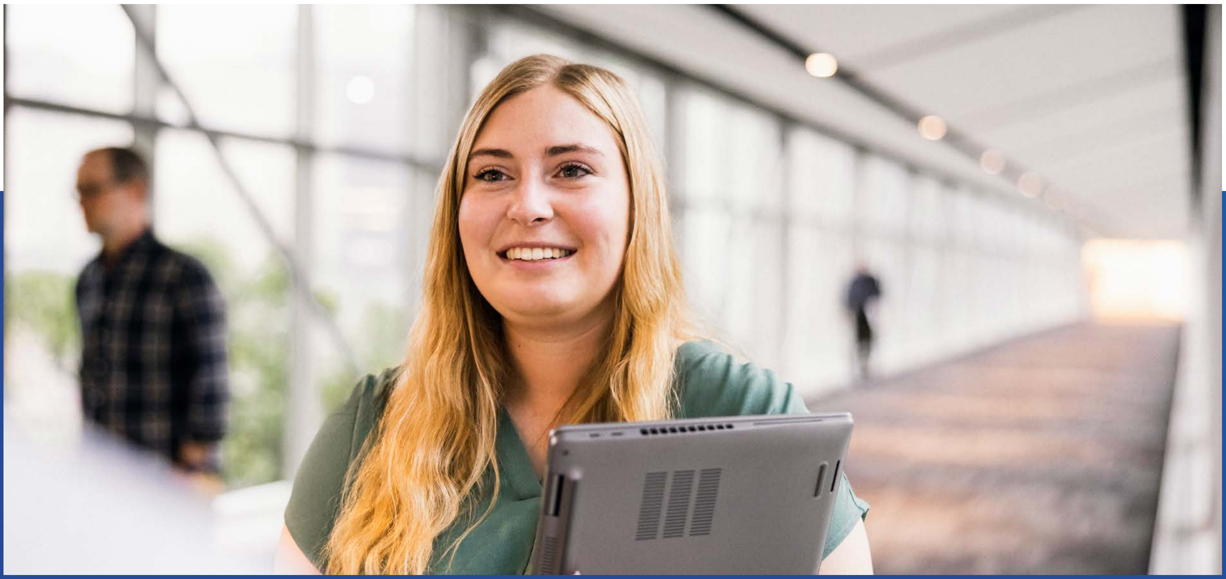
Act with integrity and the highest ethical standards
The Code helps us understand the details of how we live out our core values. If you're faced with a decision without a clear course of action, ask yourself:

- Will my decision reflect our core values?
- How would the decision make customers, co-workers, family, and friends feel about Principal and me?
- Am I willing to be held accountable?

Considering these questions can help us make sure we continue to operate in an ethical and legal manner.

Understand and manage risks related to your job
Risk is the possibility of events and/or decisions disrupting our strategy, impacting our financial results, or negatively impacting our reputation in the market and among key stakeholders like customers and investors. Like all financial services companies, we're exposed to a wide variety of financial, pricing, operational, and business risks. Managing these risks is a part of everyone's job. Analyze decisions and possible results. Make sound judgments about the risk and reward trade-offs of business decisions.

Report concerns
It's important to report activities that you believe may violate this Code. Prompt reporting may allow us to avoid or mitigate serious harm to our business or others. See "Speak up".



Notice to employees

Don't have access to links in this Code?
If you are in a location that doesn't have access to links within the Code, corporate policies and any significant policy changes will be communicated to you either by your leader or your local legal or compliance contact.

Nothing in this Code prevents you from reporting potential violations of law to relevant government authorities.

Certification
All employees are responsible for annually certifying that they have read this Code and agree to act in ways that meet our principles of integrity and our ethical expectations.

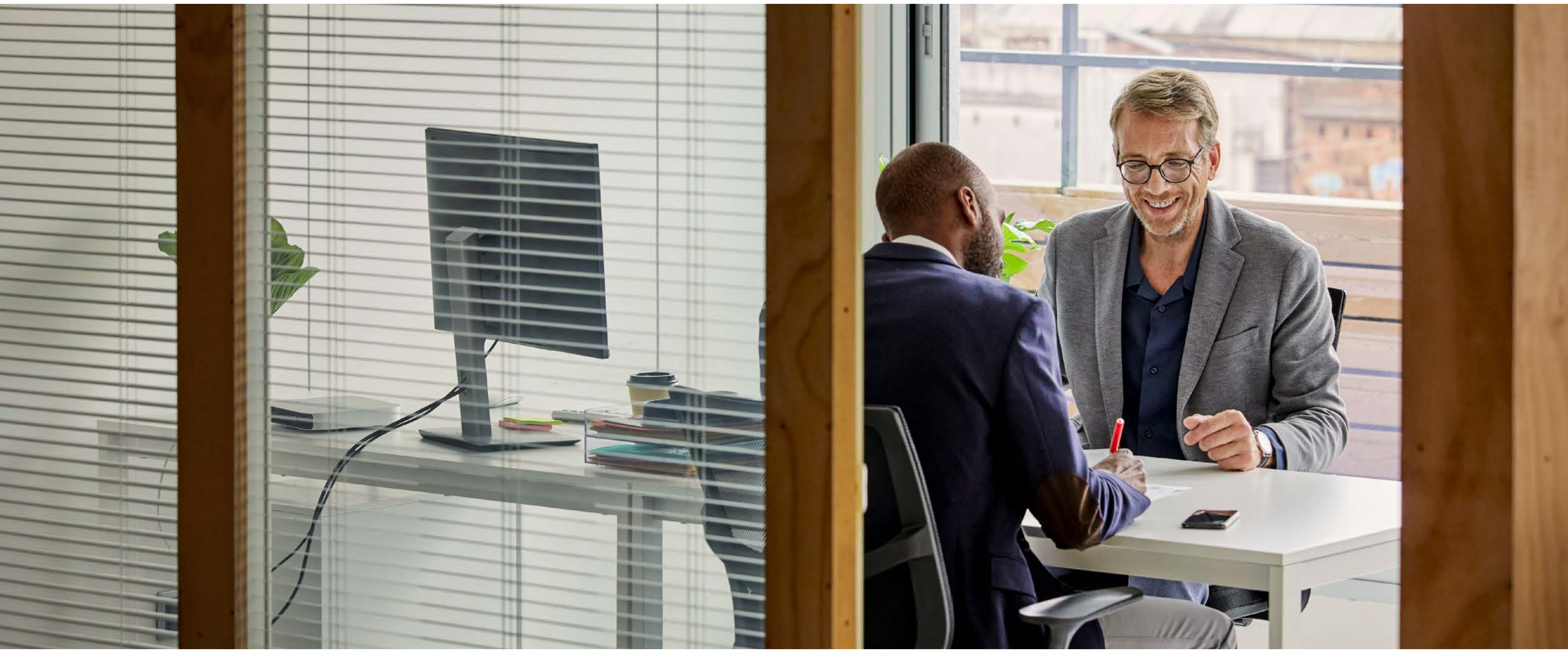
Consequences of violating the Code
Violating this Code can put our company at risk. Failure to follow the Code will result in appropriate disciplinary action, which could include losing your job or relationship with Principal.

U.S. specific
You don't need approval for posting or distributing information for activities protected by the National Labor Relations Act during non-work time and in non-work (common) locations.

Additional responsibilities for leaders

While we all must follow the Code, leaders have additional expectations to:

- Promote awareness of the Code and other enterprise policies and standards to make sure employees understand and follow them.
- Set a good example by acting ethically and with integrity and encouraging this behavior in others.
- Create an open and honest atmosphere that encourages others to speak up without fear of retaliation. Encourage employees to express their ideas, ask questions, and raise concerns.
- Handle employee concerns with respect and appreciation. Share information only with those who have a need to know to investigate and address the concern.
- Recognize that failure to follow our Code could have significant negative impact on our reputation. Identifying and reporting potential risks before they become incidents or crises is a key leadership role.
- Understand how to escalate issues or concerns to the appropriate areas, if needed.



Additional policies and standards

No set of documents can cover every legal or ethical question. You may encounter situations where your ethical obligations may not be clear, or where you're not familiar with the relevant body of law. When a decision isn't clear, you're expected to ask for help in making the right decision.

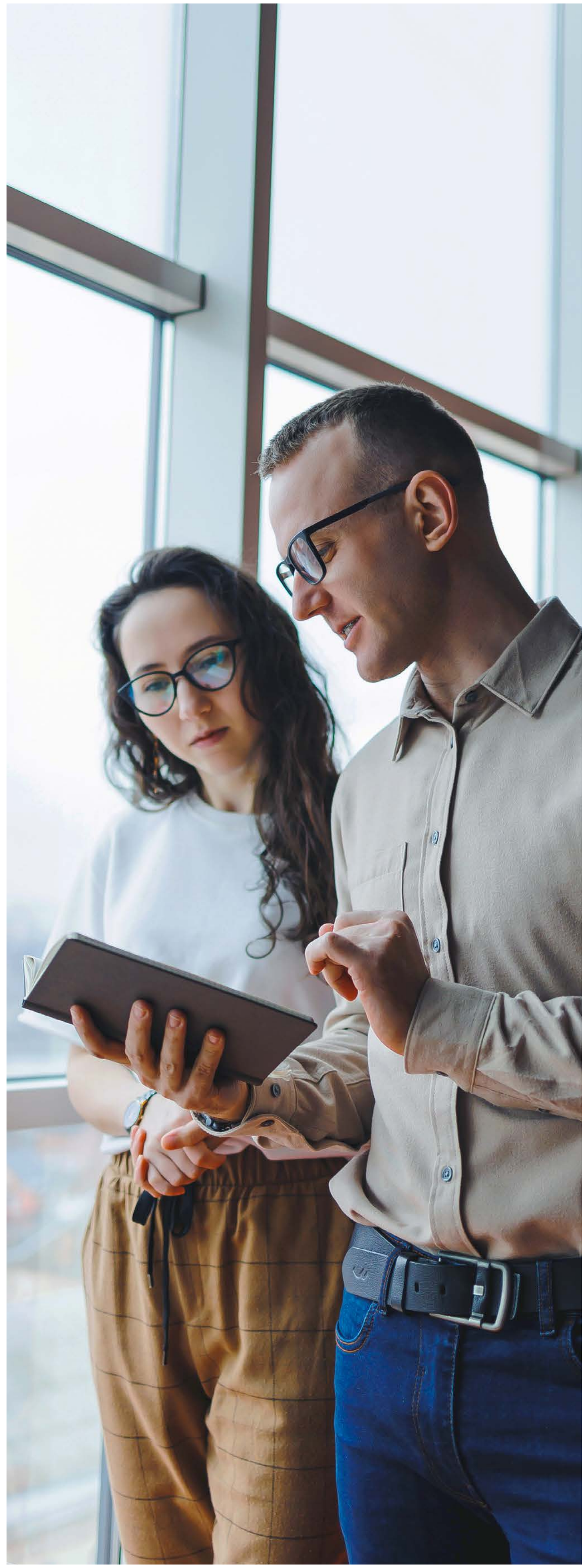
Enterprise policies and standards on Policy Central provide additional guidance on many of the topics included in this Code. You're responsible for acting in a way that aligns with this additional guidance, including any future updates.

Some Principal business areas have additional policies and codes of ethics to guide employees in situations that might come up in connection with their particular business activities. It's expected that you'll stay familiar with and follow any policies and codes specific to your role and location, in addition to this Code.

Waivers

Any waiver of this Code would be granted only under exceptional circumstances. In addition, any such waiver for a director or executive officer requires a review by our Audit Committee, approval by the Board, and disclosure on our website (www.principal.com).

> You may encounter situations where your ethical obligations may not be clear, or where you're not familiar with the relevant body of law. When a decision isn't clear, you're expected to ask for help in making the right decision.



Speak up

Unethical, illegal, or irresponsible acts can cause serious loss or harm to our organization, our employees, and our customers. Help prevent these activities and preserve our culture of integrity.

If you suspect it, report it. All reported matters are taken seriously and fully investigated. You don't have to be certain that an inappropriate activity has occurred. We have teams with the skills and resources to investigate situations to determine if a violation has occurred. Prompt reporting may allow our company to avoid or mitigate serious harm to our business or others.

Examples of concerns to report:

› Fraud
› Criminal or illegal activity
› Unethical behavior
› Bribery and corruption
› Conflicts of interest
› Accounting irregularities or falsifying accounting records
› Inappropriate sharing of confidential or customer data

If you suspect unethical or fraudulent activity, there are multiple options for reporting your concerns.

Contacts

You can reach out to:
- Your leader
- Your business area's compliance contact, the Enterprise Chief Ethics and Compliance Officer, or your local legal or compliance contact
- Your employee relations consultant or local human resource representative
- A member of the Corporate Special Investigations Unit (CSIU)
- The Ethics Hotline through a phone or online report, both of which allow anonymous reporting:
  - In the U.S., call 866.858.4433 (staffed 24/7) or submit an online reporting form
  - Outside the U.S., submit an online reporting form (or call your local hotline number, if applicable)

If you have a fraud concern to report on behalf of a customer:
- Report these using the Investigation and Privacy Incident Reporting Form

If you have questions about this Code, you may:
- Use any of the options listed above
- Submit questions to CorpPolicyReview@principal.com.

For matters covered in your location's employee handbook:
- In the U.S., visit My Service Portal.
- Outside of the U.S., consult with your local human resources representative.

Reporting suspected violations

Reporting Globally. When using the Ethics Hotline in countries outside of the U.S., reporting of certain incident types may be limited in some locations due to local laws.

Reporting anonymously. In most countries, the law allows reports to be made anonymously. Concerns submitted anonymously (through the Ethics Hotline 866.858.4433 or the online reporting form) go directly to a third party not affiliated with Principal. The third party collects the information, creates a report, and sends it promptly to the Corporate Special Investigations Unit (CSIU) for assignment to a Principal team member for investigation. You can then maintain anonymity and continue to provide ongoing information to investigators.

Performance-related issues. For performance-related issues, such as a co-worker working overtime without appropriate approval, wearing inappropriate attire, repeatedly surfing the web or texting on company time, or generally not being productive, it is more appropriate to report directly to a leader or Human Resources.

Frequently asked questions about reporting

If my leader asks me to do something that I think violates this Code, what should I do?

Never do anything that you believe violates this Code. Express your concerns directly to your leader. If you're unable to do so, or you get an answer you feel is inaccurate or unacceptable, speak with another leader or report your concerns using any of the options listed in this Code. See Contacts.

What happens after I report a concern?

All reports are taken seriously and investigated by the CSIU with assistance from various areas, including Human Resources, the Law Department, Enterprise Safety and Security, and external investigators to determine whether the concern is substantiated. We don't tolerate violations of the Code by employees or people outside of the company, and we take appropriate action against those who violate the Code. The Enterprise Chief Ethics and Compliance Officer oversees investigations and responses to concerns, and reports investigations results to the Audit Committee of the Board. A key factor to consider is the more specific you can be with details, people, and timeframes related to your concerns, the more accurate and thorough the investigation can be.

How am I protected from retaliation for reporting a concern?

Reported concerns are treated confidentially. Principal won't retaliate against any employee for reporting in good faith suspected unethical conduct or violations of law as stated in our Whistleblower policy. Retaliation against an employee for reporting an issue in good faith is itself a violation of our Code. If you know or suspect that retaliation has occurred or is occurring, you should report it.

I understand that the Ethics Hotline and online reporting form provide an option for reporting anonymously. However, can't the company use today's technology to track back to my phone number or computer?

No. Principal contracts with a third-party service provider to provide the Ethics Hotline and online reporting. The service provider collects the information, creates a report, and sends it to the CSIU for assignment to a Principal team member for investigation. Principal doesn't have access to information about the phone or computer used to report a concern. The third-party service provider is contractually not allowed to provide any identifying information if a person has elected to remain anonymous.

If I report anonymously, how will I know if anything was done with my report?

When reporting anonymously, please use the case number and password provided to see if the investigator has additional questions. You can also provide an email address to receive notification if the investigator has additional questions or follow-up. This email address is not attached to the report content and is not visible to investigators or anyone at Principal. The investigator will post a response when the investigation is completed. While we can't always share the full results of an investigation due to confidentiality concerns, please know that all reports are taken seriously and are fully investigated.

Working with business partners and customers

Everything we do keeps the best interests of our customers, employees, and shareholders in mind. We are an ethical, trustworthy company at all times and in every interaction we have with our business partners and customers.

Highlighted topics:

› Fair dealing

› Competition laws

› Global Sourcing and Supplier Management

› Customer complaints

› Audits and outside exams

Start with the customer

Do what's right

Own what's next

Invest for our future

Fair dealing

We're proud of our outstanding reputation of integrity in the marketplace. That's why we want to make sure we accurately and truthfully represent the products and services we offer.

Your role

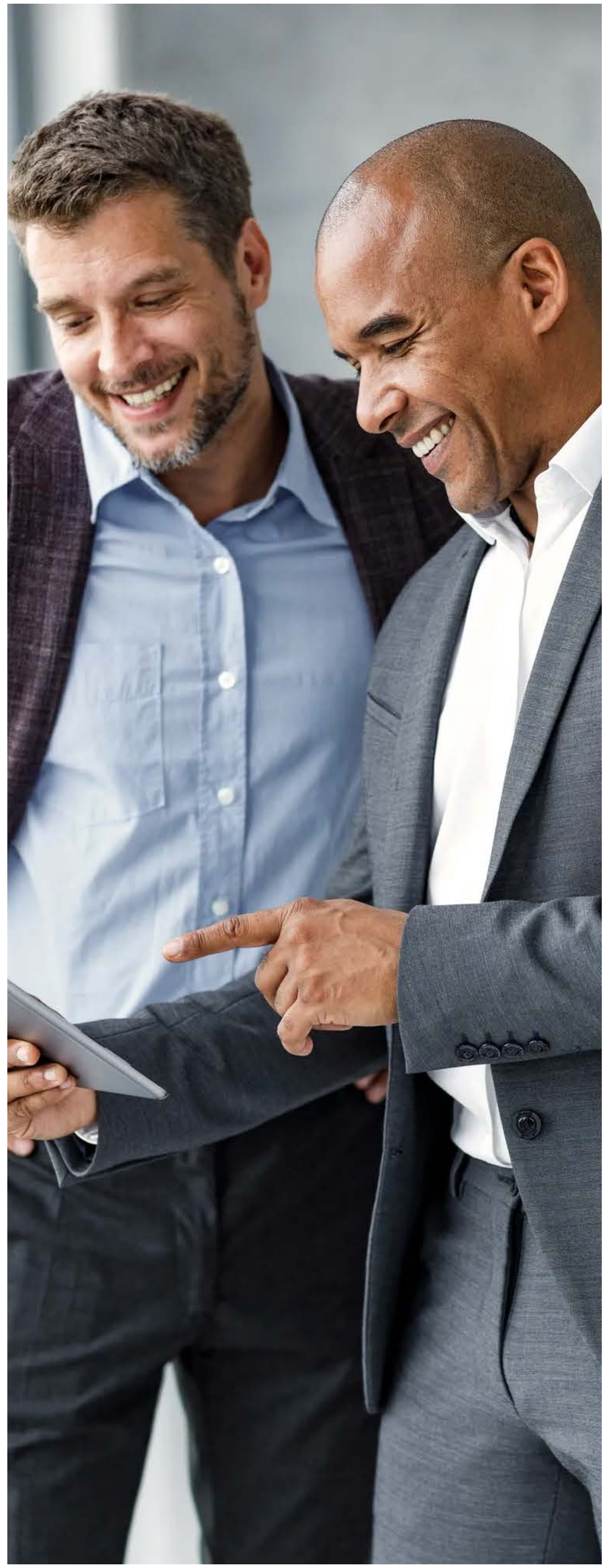
- Deal fairly with our customers, suppliers, and competitors.
- Share truthful facts about what makes our products great. Don't misstate the facts, provide misleading impressions, or make false claims about our capabilities or our competitors to gain an advantage.
- Never take unfair advantage of anyone through manipulation, concealment, abuse of confidential information, misrepresentation, or any other unfair business practice.

Competition laws

As a company, we want to outperform our competitors. But we want to do it fairly and honestly. We're committed to complying with all competition (antitrust) laws in every jurisdiction where we do business.

Your role

- Don't discuss or make agreements with competitors about issues related to non-public, competitively sensitive information (including but not limited to price), or about refusing to do business with another individual or company.
- Never communicate with competitors about or enter into any agreements to compare or coordinate bids, or to refrain from bidding.
- Don't communicate about, or enter into any agreements with, competitors to restrict or allocate sales (such as by customers, products, or territories). In addition, don't agree to avoid recruiting or hiring their employees.



Global Sourcing and Supplier Management

We want to work with companies that share our beliefs and treat their customers and employees with integrity. We also want to do right by our suppliers while making sure they follow the same standards we hold our business to. That's why we:

- Have a fair and objective process for choosing the suppliers we work with.
- Conduct thorough due diligence of suppliers before entering into a contractually binding agreement with them.
- Minimize potential risks during contract negotiations.
- Ensure contracts are fully executed before a supplier delivers products or begins providing services.
- Verify approval authority for contracts is aligned to the appropriate level of risk and/or spend.
- Determine if a purchase must go through a competitive bid or rebid process.
- Maintain an electronic record of contracts and managed suppliers.
- Actively and consistently monitor and manage risks and the performance of our suppliers during the life of the contract.

Your role

- Work with our Global Sourcing and Supplier Management departments or your local procurement or legal contact, so they can help you select a supplier and negotiate a contract with them.
- Follow our standards for executing contracts with suppliers and for managing supplier performance.
- Assess the risk involved with the supplier you want to work with and get the appropriate approvals to make sure the risk is acceptable.

Managing our suppliers

Effective sourcing and supplier management requires a collaborative effort between sourcing and supplier management professionals, legal counsel, business partners, risk management professionals, and senior business leaders. Our suppliers are managed by trained and qualified supplier and engagement managers, who monitor risks related to each engagement and evaluate the supplier's performance under the contract. Their oversight follows our supplier management governance model, which sets the minimum expectations and provides guidance for assessing, monitoring, and managing supplier risk and performance. Note that local regulations may impact our standard processes for monitoring and managing suppliers.

Customer complaints

Putting our customers first and making sure they are treated fairly is at the heart of what we do. Customer complaints give us valuable information about our business practices and the needs and expectations of our customers. The way we handle complaints helps build and maintain positive business relationships with our customers.

Important things to know:

- A complaint can be received verbally (in person or by phone) or in writing (by email, through social media, or in letters or similar correspondence).
- Regulators may define a "complaint" differently, so what constitutes a customer complaint for one business area may differ from other areas.
- Some jurisdictions and products have differing legal requirements regarding the handling of customer complaints, including reporting obligations.
- Business areas analyze customer complaints to identify systemic or recurring problems. If problems are identified, the business area takes action to address the problem and implements controls as needed.

Your role

- If you encounter a situation in which you believe a potential customer complaint has been made, immediately provide this information to your business area's customer Complaint Contact (if applicable) or your leader to make sure the complaint is recorded, resolved, and reported. Remember —some complaints have regulatory response deadlines so addressing issues in a timely manner is important.
- Share customer complaints with others only on a "need to know" basis—and follow any relevant data protection requirements.

Audits and outside exams

Periodically, parts of our business are subject to audits or examinations. We cooperate fully with these reviews whether they are conducted by our internal audit area or outside entities such as regulatory authorities or our external auditor.

Your role – internal audits

- Transparency and responding timely to internal audit requests are key to supporting Internal Audit's role in helping management identify gaps and improve the effectiveness of risk management, control, and governance processes.
- You must not place Internal Audit in a position that could impair its ability to carry out internal audits in an unbiased manner.

Your role – external audits/exams

- Notify your leader before responding to ensure proper coordination.
- In the U.S., consult with a member of the Law Department, Government Relations, or Compliance. Outside of the U.S., consult with your local legal or compliance contact.
- Contact Internal Audit or the Law Department if you receive requests for internal audit reports or workpapers so appropriate documents can be reviewed and prepared.
- Cooperate fully with all appropriate requests for information. Provide a timely response and information that is accurate to the best of your knowledge.

Conflicts, bribery, and corruption

We're committed to following the laws and regulations of every country and community we do business in. Conflicts of interest, bribery, and corruption have no place in what we do.

Highlighted topics:

› Conflicts of interest

› Gifts and entertainment

› Bribery and corruption

› Political activity

› Anti-money laundering

› Economic sanctions

› Anti-boycott

› Insider trading

Start with the customer

Do what's right

Own what's next

Invest for our future

Conflicts of interest

We make our business decisions based on sound business judgment, not on any employee's personal interest or gain.

Your role

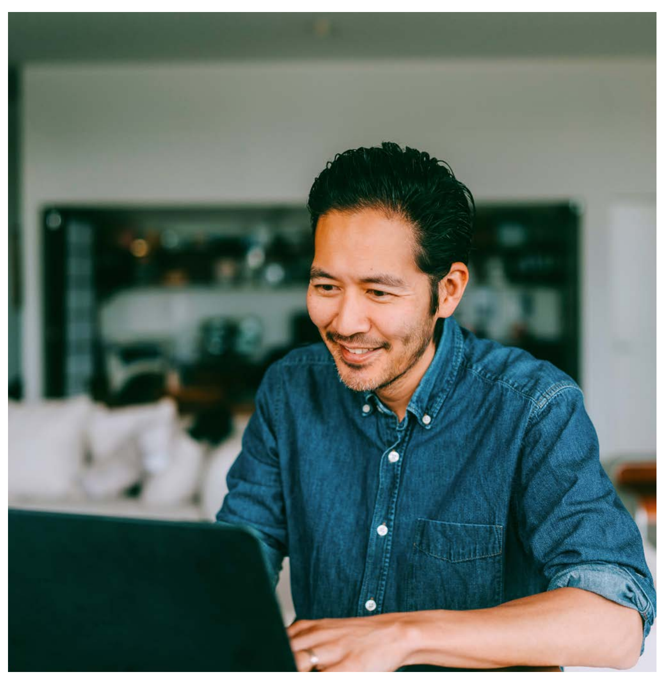
- Avoid situations that may create, or even appear to create, a conflict between your personal interests and the interests of our company.
- Be familiar with the Conflicts of Interest policy ("COI Policy"), which applies to all employees at all levels.
- If you believe you might be involved in an activity or relationship that could present a conflict with Principal, seek review and approval of the activity or relationship from your leader and compliance area in accordance with the COI policy.
  - Employees who hold the title of Vice President or above (or equivalent title as determined by Human Resources) must also work with their business unit Chief Compliance Officer to obtain the approval of their activity or relationship from the Conflicts of Interest (COI) Committee.
- If your activity or relationship is approved, please remember the following:
  - Approvals are subject to an annual review,
  - If the facts that an approval was granted under have changed, the employee must share the new information with their leader and compliance area for review,
  - The conflict should be disclosed on the annual Conflicts of Interest questionnaire if you're required to complete one, and
  - The conflict must not interfere with your job responsibilities and you may not use company resources.
- It's impossible to anticipate all circumstances and conditions that might create a conflict of interest. If in doubt, talk to your leader.

If you're approved to serve on an outside board or other governing body, you should make it clear that, unless Principal has asked you to serve, you're serving in a personal capacity and not at the direction or request of Principal. You must not participate in any decisions involving Principal products or services.

What are some examples of conflicts of interest?

Here are a few activities that are not allowed or require careful consideration:

- Allowing decisions in your capacity as a Principal employee to be influenced, or appear to be influenced, by personal or family interests or friendships.
- Having a financial interest in, or performing work for, another entity that is a customer, supplier, or competitor of Principal.
- Using your business relationships or connections for personal gain.
- Serving on a board of directors or other governing body for an organization that does business with or competes with Principal.
- Using company property, information, or resources for personal or outside activities.
- Having an outside job that interferes with your ability to perform your job responsibilities at Principal or involves the use of company time or resources.



Gifts and entertainment

We don't accept or provide any gift or entertainment (including travel) that might influence, or appear to influence, any business decision.

Your role

- Gifts and entertainment activities must be legal and shouldn't be frequent or extravagant.
- Avoid any gift or entertainment activity that may create an actual or perceived conflict of interest or the appearance of impropriety.
- Don't offer any gifts or entertainment, regardless of value, to government officials without advance approval of Government Relations (U.S.) or the appropriate local legal or compliance contact.
- Know reporting requirements and limits for giving and receiving gifts and entertainment. These can vary depending on your business area and location. Refer to the gift and entertainment requirements and limits applicable to your location or contact your compliance or legal contact for further guidance.

I purchased two tickets for a sporting event to spend time with my client. The client asked me if they could bring their spouse. Since the event is sold out, may I give both tickets to the client so their spouse can attend in my place?

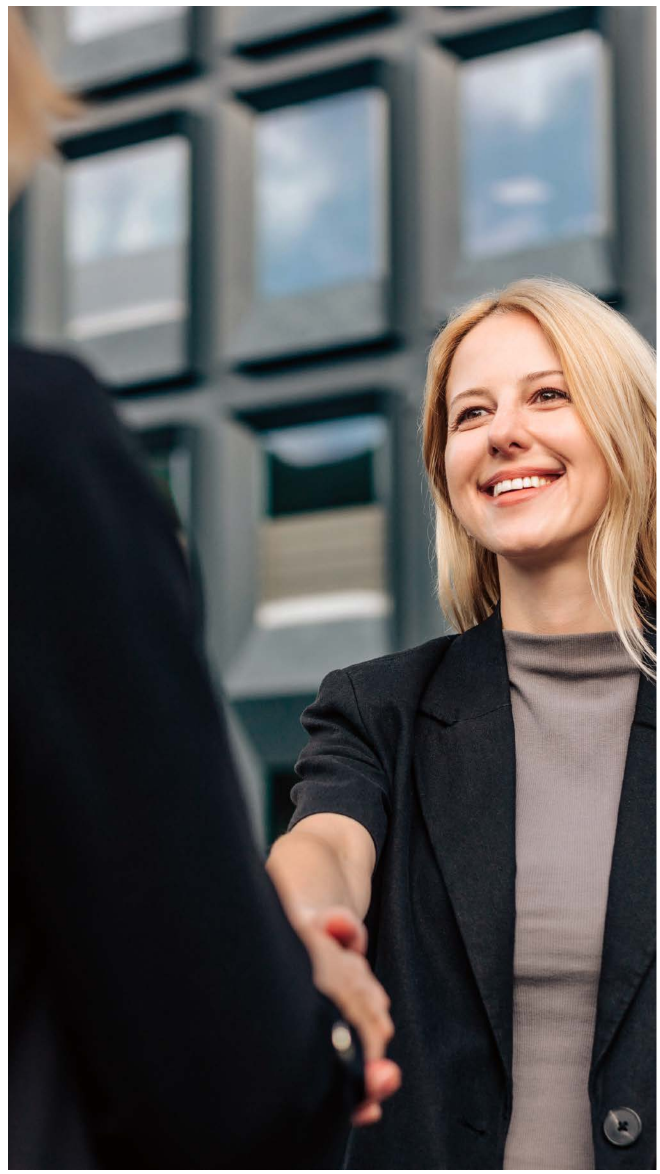
If you don't attend the event with the client, the tickets would be considered a gift, instead of business entertainment. Therefore, the total value of both tickets must fall within the gift limits.

What is the monetary limit for a business gift?

Refer to the gifts and entertainment standards for details regarding limits. Some business areas have adopted their own gift policies and standards due to business needs and legal requirements. Consult your business area's requirements before giving or accepting any business gift.

I want to give a client a gift that exceeds the monetary limit. Is the gift permissible if I pay for it myself and don't request reimbursement from the company?

No. Monetary limits apply whether or not you request reimbursement from the company.



Bribery and corruption

Bribery is unethical, illegal, and against our company values. We don't seek to influence others by offering, paying, or receiving bribes or kickbacks, or by any other means considered unethical, illegal, or harmful to our reputation of honesty and integrity. Bribery can expose our company and employees to fines or other penalties like imprisonment.

Your role

- Decline any opportunity that would risk our ethical principles, reputation, or cause us to violate the Foreign Corrupt Practices Act (FCPA), the U.K. Bribery Act, or other applicable anti-bribery and anti-corruption regulations. Many anti-bribery regulations such as the U.S. FCPA apply to every Principal employee regardless of the country the employee works in.
- Don't give or offer anything of value that could be perceived to be an attempt to improperly influence a decision, secure an advantage, avoid a disadvantage, or to obtain or retain business.
- Be especially cautious when interacting with government employees or officials. Reasonable corporate hospitality that is acceptable with other business partners may not be allowable due to their status as a government official.
- If a person or company you're doing business with offers you a bribe, you should decline it and immediately report it to your local legal or compliance contact.
- When in doubt, double check: If you're offered something of value and you're not sure if you're allowed to accept it, double check the gift and entertainment policy. You can also check with your leader or your compliance or legal contact.
- If you do accept or offer something of value that is permissible under Principal policy and applicable regulation, it must be recorded completely and accurately. Include receipts where required.
- Do not use a third party to make improper payments.

We're trying to get the business of a state-owned enterprise. One of their employees assured me that it would be looked upon favorably if we make a contribution to their favorite charity. Since the contribution doesn't benefit the employee personally, would this be a bribe?

This could be considered a bribe. A bribe is not only cash. A bribe can include providing jobs or internships for employees of state-owned enterprises or making charitable contributions suggested by employees of state-owned enterprises. Check with your local compliance or legal contact before making any such agreements or payments.

Anti-bribery and corruption policy

A government official is any:

- individual elected or appointed to a governmental entity regardless of rank,
- official or employee of a government,
- official or employee of a company wholly or partially owned or controlled by a government or a government entity. This includes state-owned entities such as sovereign wealth funds.,
- candidate for political office,
- political party or official of a political party, or
- person acting in an official capacity for any of the above regardless of rank or position.

Political activity

We support and respect the rights of employees to participate personally in the political process. Our company doesn't make corporate contributions to political campaigns. Since campaign laws are strict concerning the use of corporate resources to support or oppose a candidate, it's important to keep a clear distinction between personal and work- related political participation..

- Our interactions with government officials are conducted with integrity and comply with laws and regulations.
- We follow established limits and reporting requirements for employee and political action committee contributions.
- Only certain employees are allowed to lobby on behalf of Principal to educate government officials about how legislation and regulations may affect our customers, shareholders, industry, and our company.

Your role

- Pre-approval is required for any gift, entertainment, or travel offered to a government official regardless of value or jurisdiction. U.S. employees: check with Government Relations. Employees outside the U.S: check with Government Relations or your local legal or compliance contact before you offer anything.
- Keep detailed records of your contact with government officials and public entities if you're talking to them about obtaining or retaining government business.
- If you participate in political activities on a personal basis, use your own resources and non-work time. Use your personal email, your personal computer or phone, your own supplies, and do these things in a non-work location.
- In the U.S., if your personal political activities require time away from work, please review the Public Office Leave section of the Employee Handbook for further instructions and requirements. For all other locations, consult with your compliance or legal contact prior to engaging in these activities.

Our business area plans to invite a speaker to a future department meeting who happens to be a government official. Are there any special considerations we need to keep in mind?

Yes, the person's position as a government official requires special scrutiny. In the U.S., pre-approval from Government Relations is required for any gifts, entertainment, or travel provided to a government official. If outside the U.S., check with Government Relations or your local legal or compliance contact before you offer anything. In most instances within the U.S., no gifts, entertainment, or travel are allowed to be given to a government official. Even if no gifts, entertainment, or travel are intended to be provided to an elected official invited to speak at a department meeting, prior to extending the invitation, pre-approval is required.

Corporate political contributions policy

Pay-to-play: In the U.S., certain employees must preclear their personal political contributions for compliance with SEC, state, and local pay-to-play laws. Generally, this includes officers, sales employees and their managers, and investment advisor employees. Employees required to preclear their personal political contributions are notified directly. If you 're unsure, contact your compliance area.

Anti-money laundering (AML)

We're committed to preventing money laundering and the financing of terrorism. We maintain anti-money laundering and other programs to detect suspicious transactions involved with these activities. We report such transactions or activities in a timely manner to the proper authorities.

Your role

- Be familiar with your business area's:
  - procedures for customer identification and verification (including know your customer processes) for opening new accounts and servicing existing accounts.
  - procedures relating to the detection of red flag activities that may require special attention.

Anti-money laundering policy

Red flag examples

- Attempts to open an account with false information.
- Transactions using cash, money orders, cashier's checks, cross border wire transfers, or other cash equivalents.
- Making an overpayment and then requesting a refund.
- Payments or withdrawals that are unusual or inconsistent with a customer's business.
- Unusual fund transfers to or from individuals or countries unrelated to the customer or transaction.
- Transactions that might appear to be structured to evade recording or reporting requirements.

Economic sanctions

We're committed to complying with economic and trade sanctions and terrorist financing laws applicable to our business. Sanction laws help fight against various threats such as terrorist activity, drug trafficking, proliferation of weapons of mass destruction, and other illicit activities.

In connection with sanctions and terrorist financing laws, lists are provided of countries, groups, and individuals with whom transactions may be prohibited or restricted. To aid in compliance, we have systems in place that compare the names of Principal customers, business associates, vendors, and payees against these lists.

Your role

- Familiarize yourself with and follow any sanction procedures that apply to your job.
- Don't do business with customers whose money you believe might have come from criminal activity or a sanctioned source.
- Watch for any activities that raise a red flag and report them to compliance or your leader.

OFAC/sanctions policy

Anti-boycott

The U.S. government monitors and, in certain cases, penalizes U.S. companies for engaging in certain international boycott activities. Anti-boycott laws help prevent U.S. companies from being used to implement foreign policies of other nations which run counter to U.S. policy..

We don't participate in prohibited or unsanctioned boycotts, and we require affiliates to promptly report any such requests to do so. In addition, we report commercial activities in, or related to, certain countries as required by some boycott laws.

Your role

If you believe you have been asked to participate in a boycott:

- Don't cooperate with the request.
- Immediately contact a member of the Law Department or your compliance contact.

What is a boycott request?

A request, as a condition of doing business, to discriminate against a person or company from a target country comprised of or affiliated with a particular nationality, race, or religion.

Insider trading

It's against the law to purchase or sell securities if you have material, nonpublic information about those securities. It's also against the law to share that information with others or to recommend purchasing or selling stocks or other securities based on that information.

Your role

- If you have access to any material, nonpublic information about our company, don't share it with others or use it – or cause others to use it – to buy or sell our stock or other securities.
- Don't purchase or sell the stock or securities of any other company when you have material, nonpublic information about that company. This applies no matter what role you have. And it applies to trading stock or other securities of others we work with—our customers, our suppliers, or our partners, for example.

I don't work with stocks or securities in my job. Do prohibitions on insider trading apply to me?

Yes, anyone with knowledge of confidential, material information can violate insider trading laws if they disclose material non-public information to third parties who may then trade stock or other securities based on that information or if they themselves trade stock or other securities based on that information. Even during casual conversations with family and friends, you must exercise caution and not disclose any information classified as company confidential

What's material information?

Any information that a reasonable investor is substantially likely to consider important in making an investment decision. A few examples of material information include expected earnings for a given quarter, information about a potential merger or divestiture, revisions to financial statements, or changes in the board of directors, corporate officers, or our public accounting firm. If in doubt about whether information is material, please reach out to the Law Department.

Information management and security

Data is one of our most important company assets. To protect it, we must maintain its confidentiality, integrity, and availability. This includes safeguarding data against unauthorized use, modification, disclosure, or destruction.

Highlighted topics:

- Information security
- Privacy
- Artificial intelligence
- Records management

Start with the customer

Do what's right

Own what's next

Invest for our future

Information security

In today's world, threats - including cyberattacks - come from around the globe. We're committed to protecting company, employee, and customer data and making sure it's accurate and available for employees who need it for legitimate business purposes. We protect data based on its classification to ensure it's handled appropriately.

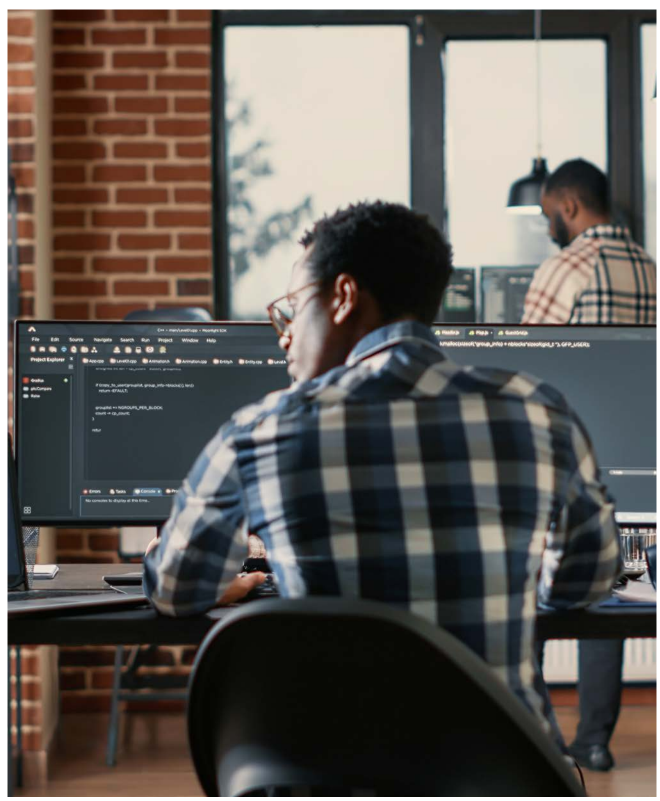
Your role

- Access or attempt to access data and technology assets only when authorized to perform your job duties.
- Share the minimum data needed for legitimate business purposes.
- Provide customers with account data only when authorized to do so and after verifying their identity using current business area requirements.
- Classify and label company data appropriately so others know how to properly share, protect, and use it, regardless of format or storage location.
- Protect data according to its classification and business purpose whenever and wherever you're accessing and using it.
- Use only approved systems and methods for storing, sharing, and transmitting company data.
- Report any observed misuse or inappropriate activity.
- Complete required information security training.
- Formally acknowledge your responsibilities for appropriately protecting company information if required to do so.

Security expectations are communicated to contingent workers based on the deliverables of the engagement.

What are key actions I can take to help protect the confidentiality, integrity, and availability of data and technology assets at Principal?

- Create and maintain strong passwords; Don't share or reuse them across accounts.
- Use company-approved encryption solutions to securely send personally identifiable information outside the company network.
- Use cloud solutions only when approved safeguards and agreements are in place.
- Access company email using approved processes and/or applications on approved devices.
- Don't click suspicious links or attachments in emails.
- Report known or suspected phishing attacks via the Report Phishing button or by emailing them to abuse@principal.com or your local reporting email address.
- Lock your devices when leaving your workspace
- Secure equipment at the end of each business day when in public places or when working from home
- Stay informed about the latest cyber risks and threats.



Privacy

We're committed to being responsible stewards of the personal data entrusted to us by our customers, workers, business partners, and others. All personal data under our care must be handled lawfully, fairly, transparently, and securely.

Your role

You are responsible for protecting personal data in your day-to-day work.

- **Collect only what you need.** Only collect personal data that is appropriate and necessary for a legitimate business purpose.
- **Be transparent and purposeful.** Clearly explain how personal data will be used and only use it for that stated purpose. Complete a Privacy Assessment before implementing any new use of personal data.
- **Respect individual choices and rights.** Ensure individuals can exercise their personal data rights, including opting out when applicable.
  - U.S. Data Subject Rights Request Form
  - EU and UK Data Subject Rights Request Form
- **Keep data accurate.** Take reasonable steps to ensure personal data is accurate, complete, and up to date.
- **Limit sharing.** Share personal data only with proper authorization, consent, or as permitted or required by contract or law.
- **Protect data.** Follow security requirements, including encrypting sensitive personal data and anonymizing or masking personal data when possible.
- **Report concerns immediately.** Promptly report suspected or actual privacy incidents, including lost or stolen equipment that may store personal data.
- **Know the rules.** Understand the privacy laws and requirements that apply to your role and location. Refer to the Privacy Policy and Standards for details.
- **Complete required training.** Participate in all mandatory privacy training

How is privacy different from security?

Information security protects data from unauthorized or unintended loss of confidentiality, integrity, or availability. Privacy focuses on protecting individuals from harm that could result from how we use their personal data, even if that use is authorized. Using personal data lawfully, fairly, transparently, AND securely protects Principal and the individuals who trust us with their personal data.

Privacy policy

Reporting a privacy incident

If you believe personal data has been improperly collected, accessed, used, or shared, report it immediately by contacting your Business Privacy Representative or submitting the Investigation and Privacy Incident Report form. Prompt reporting helps Principal reduce risk and meet legal and regulatory obligations.

Personal data relates to an identifiable individual, and may identify them directly or indirectly.

Examples include:

- Name
- Address
- Phone number
- Email address
- Birth date
- Online identifiers, such as IP address
- Financial profile
- Credit card data
- Government assigned identity numbers
- Passport number
- Employment data

Artificial intelligence (AI)

At Principal, we're building artificial intelligence into the foundation of our enterprise to make financial services smarter, faster, and more personal, while maintaining the trust that defines who we are. Our AI strategy is designed to create real-world value: from retirement solutions to asset management, from fraud detection to personalized communication. We use AI to amplify enduring human capabilities. Guided by our Ethical and Responsible AI (ERAI) framework, AI use cases are inventoried and evaluated for risk and monitored appropriately to maintain fairness, transparency, and compliance with our AI policies and standards

Your role

- Know and follow Principal's AI policies and standards.
- Complete required training to stay current on expectations on how to effectively use, develop, deploy, and procure AI solutions.
- Use AI only for approved business purposes and within intended limitations; maintain human oversight and validate outputs before using them in your work.
- Protect data: do not enter or expose confidential (company/customer), proprietary, personal/sensitive, or internal-use-only information in any AI tool unless approved for that category of information.

Records management

We retain records created for our business activities for the time necessary to meet business, legal, and regulatory requirements.

Your role

- Create, retain, and destroy records according to the records management policy.
- Destroy records securely and promptly after the termination of the retention period, unless new business needs or legal obligations are identified.
- Suspend destruction through legal holds when necessary due to litigation, government investigation, audit, or instruction from the Law Department and resume destruction of records once the hold is released.
- Ensure appropriate oversight of the retention and destruction of records managed or retained by third parties on our behalf.
- Complete required training courses related to records management.

A record is any information created, received, and maintained as evidence of business activities or to meet legal obligations.

Financial management and reporting

We're dedicated to communicating financial results that completely and accurately reflect our underlying business activities in compliance with legal and regulatory requirements. We maintain effective internal controls, align expenses with revenues, and make sound business decisions based on complete analysis with the proper consideration of short and long-term risks.

Highlighted topics:

› Accurate and transparent financial information
› Protection and proper use of company assets
› Sharing material information
› External auditors

Start with the customer

Do what's right

Own what's next

Invest for our future

Accurate and transparent financial information

We're committed to transparency in our financial reports. Our reports and accompanying disclosures are truthful, complete, consistent, fairly presented, timely, and understandable. We prepare our financial information following legal and regulatory requirements.

We also establish and maintain a robust system of controls to help ensure the integrity of our financial reporting processes and financial statements.

Your role

- When creating, transmitting, or entering information into company financial records, do so accurately, completely, and with appropriate supporting documentation.
- Ensure financial transactions are properly authorized.
- Ensure physical assets and financial information are appropriately safeguarded.
- Perform controls you are responsible for according to established procedures in a timely manner. Follow up on exceptions immediately.
- If you discover a control breakdown or an error in our financial statements, report it to your leader or other relevant management immediately.

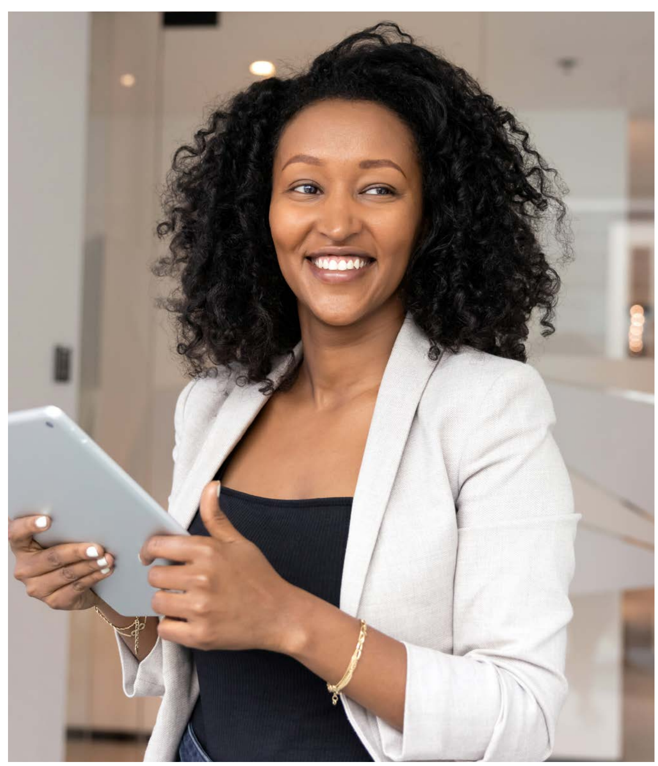
What does "accurate and transparent financial information" mean?

It means we need to be honest, accurate, and open about our financial information and in the financial documents we create.

To keep our financial information transparent, you should never:

- Make entries or alter records to intentionally hide or disguise the true nature of a transaction
- Deliberately understate or overstate liabilities or assets
- Improperly accelerate or defer the recognition of expenses
- Record false revenues or record them early
- Make false claims on an expense report or timesheet
- Withhold information required to be disclosed in regulatory reports
- Falsely certify the accuracy of financial information or the effectiveness of controls we have in place

Our chief executive officer, business unit heads, and all financial personnel are held accountable for complying with this Code and our financial reporting policies.



Protection and proper use of company assets

We treat company assets with care and use them for legitimate business purposes.

Your role

- Use company resources honestly and efficiently.
- Use computers and network systems appropriately and in accordance with company policy at all times.
- When using personal devices to perform certain work-related functions, it's important to follow company policy and protect the information and data stored on or sent through these resources.

Report suspected or known loss, theft, damage, or misuse of resources immediately.

Company assets include but are not limited to:

- Physical property, such as company supplies, computers, and equipment
- Intangible assets, such as company time, company funds, confidential information (including data), intellectual property, and information systems

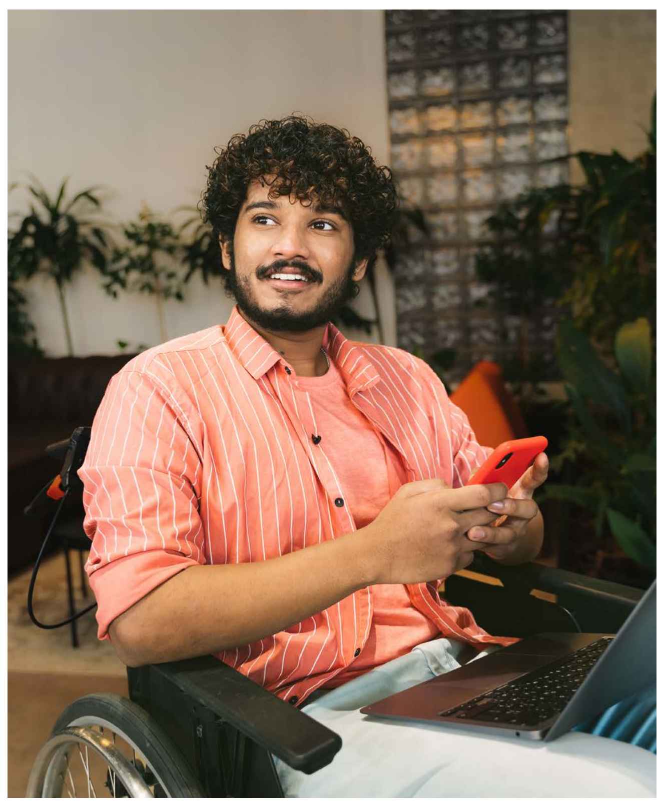
Sharing material information

Since we're a public company, disclosures about our business must be made consistently and shared broadly, so that investors have fair access to this information. The company has designated primary spokespersons to speak on behalf of the company or to respond to specific inquiries from investors, analysts, or the media.

Your role

- Don't communicate any material information externally unless you're a designated spokesperson for the company.
- You should refer any inquiry about the company from the news media, security analysts, our shareholders, and the public to the Public Relations team.

Disclosure statement



External auditors

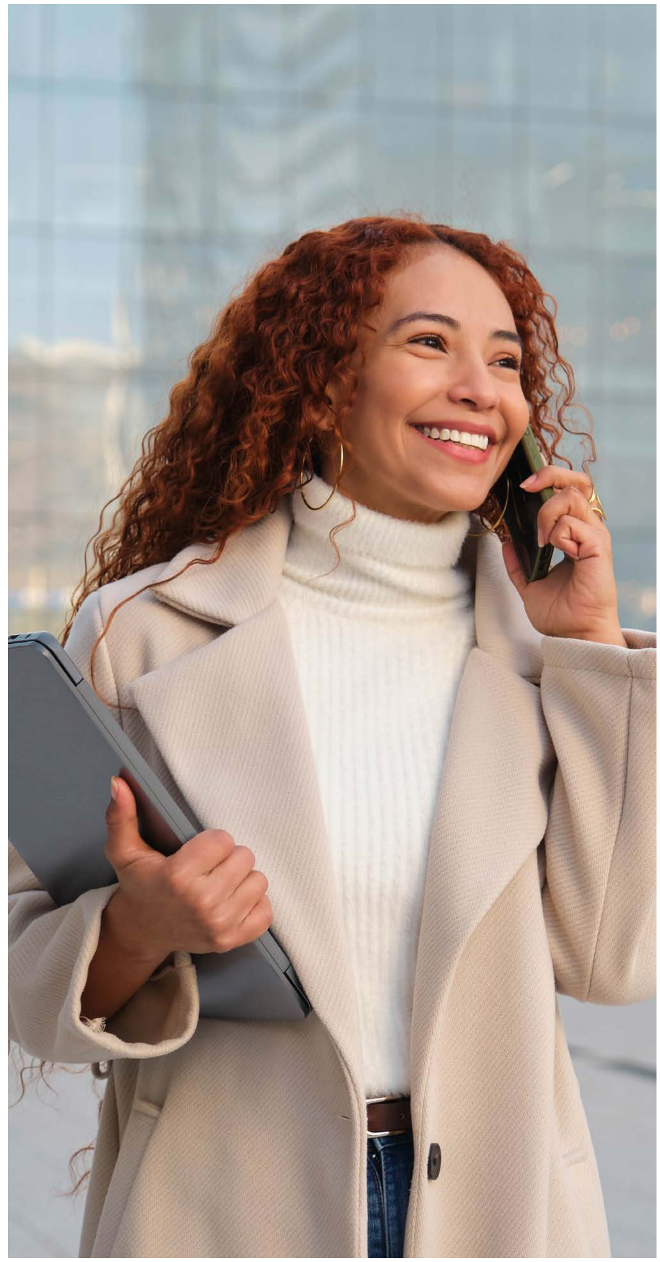
Ensuring the independence of our external auditors is critical. Our management, Board of Directors, and Audit Committee share the responsibility of maintaining this independence.

The Audit Committee of the Board of Directors selects the audit firm for Principal. To maintain audit consistency and efficiencies, all subsidiaries and affiliates should use the same financial statement auditor. Any exceptions should be discussed with the business area chief accounting officer and corporate controller.

Your role

- Cooperate fully with auditors and regulatory authorities. See Audits and outside exams.
- Work through your business unit chief accounting officer and the corporate controller to get Audit Committee approval for all proposed external audit services before you start using those services.

Before we hire staff that works for (or used to work for) our primary independent auditor, we carefully evaluate the situation for any potential independence concerns.



Fair employment practices

We're committed to providing an inclusive work environment, free of unlawful discrimination, and harassment. We also comply with all applicable employment and labor laws.

We expect leaders to champion these principles, and we hold all employees accountable for upholding them. Violations of our fair employment standards or related policies may result in disciplinary action.

Highlighted topics:

› Policies and employee handbooks
› Employment of relatives and personal relationships
› Drugs and alcohol
› Global inclusion
› Discrimination, harassment, and retaliation
› Human rights

Start with the customer

Do what's right

Own what's next

Invest for our future

Policies and employee handbooks

We have policies and expectations of employment in place to outline appropriate processes and standards of behavior for our employees to follow.

Your role

- Be sure you are familiar with your applicable employee handbook.
- Periodically review and be familiar with enterprise policies and standards.

Where to find employee handbooks and policies

- In the U.S.: Access the employee handbook on the intranet using the links below.
- If you work at a location that has its own handbook or at a location outside the U.S., contact your local Human Resources department.
- Enterprise policies and standards can be found in Policy Central on the intranet.

Employment of relatives and personal relationships

People that work at the Company must not be directly or indirectly supervised, at any level of leadership within their chain of command by a member of their immediate family or by a person with whom they have, or had, a romantic or close personal relationship. Immediate family members of non-employee directors on the Board of Directors of Principal Financial Group, Principal Funds, and Principal Bank must not be hired.

Your role

- During the hiring process, and prior to scheduling department interviews, leaders should inform Talent Acquisition or their local recruiter of any such relationships with candidates. Employees applying for internal positions should immediately notify Talent Acquisition or their local recruiter if they learn they have such a relationship with the leader (or any level of leadership within the chain of command).
- After hiring, if such a relationship is found to exist or develops between an employee and their leader (at any level of leadership), both must inform their employee relations consultant or local Human Resources department.

Drugs and alcohol

We value a healthy and safe work environment that promotes productivity and employee and customer safety. Abuse of drugs and alcohol places the work environment and our reputation at risk.

Your role

- Use good judgement and act responsibly when representing the Company or conducting business on its behalf.
- When you are representing the Company or conducting business on its behalf, don't be under the influence of alcohol, illegal drugs, or prescription drugs that aren't prescribed to you. Alcohol may be responsibly consumed in the workplace as part of an approved, Principal-sponsored event. (In locations where alcohol use in the workplace is prohibited by law or local policy, those local restrictions must be followed.)
- If you or someone on your team needs support related to drug or alcohol use, reach out to your local Human Resources contact for information on confidential resources available through the Employee Assistance Program (EAP).

Global inclusion

We're drawn to people who bring unique perspectives, passion, and expertise to help us advance the financial security and well-being of our customers, transform our growing business, and drive positive change in the communities where we live and work. As part of our collaborative culture, we prioritize inclusion, shared values, and genuine support for every employee around the world. All our employees contribute to a thriving environment of authenticity, action, and accountability—which reverberates within our company and our communities.

Your role

- Continuously grow and apply learnings from training programs to help create a more inclusive culture.
- Create a safe environment where everyone feels valued and respected.
- Review the U.S. Employee Handbook: Discrimination, Harassment and Retaliation or your local policy.

Additional note for leaders

- Make selection decisions (i.e., hires, promotions, turnover) based on job qualifications, skills, and performance.
- Evaluate performance based on the work employees do each day and other job-related requirements.
- Review the U.S. Leader HR - Policies and Laws (for leaders): Discrimination, Harassment and Retaliation or your local policies.

Discrimination, harassment, and retaliation

We believe in treating each other with respect and dignity, and in fostering an atmosphere of open communication, trust, and mutual respect. We expect that all work relationships will be free of bias, discrimination, harassment, and retaliation.

- We're committed to the fair treatment of all employees and applicants for employment. We make employment decisions based on qualifications, demonstrated skills, and achievements.
- We provide equal employment and advancement opportunity for all individuals and will make reasonable accommodations for employees and qualified applicants with disabilities.
- Harassment of any kind is determined by how others perceive your actions, regardless of your original intent. We don't tolerate verbal or physical conduct by any employee that harasses another employee or creates an intimidating, offensive, or hostile work environment.
- We don't tolerate discrimination in hiring, training, advancement, compensation, discipline, or termination.
- Retaliation includes any action that could have the effect of preventing someone from making a complaint under this policy. We strictly prohibit retaliation against anyone for raising a concern or making a report in good faith. Every employee should feel safe to speak up, and any person who retaliates is subject to disciplinary action.

Your role

As an employee, you are a steward of our culture. Your help is needed to ensure Principal remains a great place to work for all employees. You should:

- Speak out if a co-worker's conduct makes you uncomfortable. We must hold ourselves accountable to the highest professional standards, with mutual respect and fair treatment as the starting point for all our professional relationships.
- Report perceived discriminatory, harassing, or retaliatory behavior immediately to your leader or employee relations consultant or local Human Resources contact. There may be business locations in which you are required to follow specific procedures regarding these situations. You must understand and comply with local applicable employment and labor laws.
- If you are not comfortable reporting an issue to your leader, employee relations consultant, or local Human Resources contact, use the Ethics Hotline. All reports will be handled confidentially.

What is considered harassment?

Harassment is a type of discrimination that includes behavior based on a person's protected characteristic(s) that results in (1) an explicit change to the terms or conditions of employment or (2) constructively changes the terms or conditions of employment through the creation of a hostile work environment. Legal definitions of harassment vary by country, but our global standard is clear: we do not tolerate any behavior that creates an intimidating, offensive, or hostile work environment

Examples of harassment include:

- Insulting or degrading jokes, remarks, or conduct
- Sexual harassment which is conduct of a sexual nature or based on a person's sex
- Disparaging or abusive comments
- Threats or intimidation
- Offensive objects or pictures displayed in the workplace, including anything circulated through email or the intranet

Human rights

As a purpose-driven company, we respect human rights. This value is embedded in our company culture around the world.

Our commitment includes using only voluntary labor, following all applicable wage and benefit laws, not employing underage individuals in violation of any applicable child labor laws, providing a work environment that is safe, healthy, and free of harassment and unlawful discrimination, and hiring vendors who adhere to these same principles.

Principal respects and supports human rights principles as defined by the principles of the Universal Declaration of Human Rights (UDHR), the International Labor Organization's Declaration on Fundamental Principles and Rights at Work ("ILO Declaration"), the United Nations Global Compact, and the United Nations Guiding Principles on Business and Human Rights.

We will not tolerate human rights violations of any kind, including human trafficking, slavery, forced labor, and child labor. We are committed to implementing and enforcing effective systems and controls to prevent violations from taking place anywhere in our business or supply chains

Your role

- Be familiar with the Anti-slavery and human trafficking policy and the Human rights statement.
- If you suspect or have a human rights, labor, or human trafficking concern in our business or supply chain, report it.

Human rights statement

Modern slavery and human trafficking statement

If you are involved with identifying or contracting with suppliers:

- Seek out those whose corporate values are consistent with ours.
- Include an anti-slavery contract provision when the supplier is in a high-risk country and high-risk business sector.

Workplace safety and security

We value the safety and security of our employees, business partners, guests, and assets. And we want to make sure we have continuity in all our business operations.

Highlighted topics:

› Safety and security of our employees
› Site security
› Emergency management
› Business continuity

Start with the customer

Do what's right

Own what's next

Invest for our future

Safety and security of our employees

We provide appropriate programs and controls to help mitigate personnel safety and security related risks.

- We comply with all applicable safety and security laws and regulations where we operate.
- We don't tolerate any threats, acts, or the intent to commit violent acts that jeopardize, or appear to jeopardize, the safety of our employees, business partners, guests, or our physical assets.
- We prohibit the possession of weapons, in line with local governing laws, on any company or leased property, at any company-sponsored event, and anywhere company business is conducted, regardless of whether or not an individual is licensed to carry a weapon.
- We provide ways for our employees to report safety or security issues, and we have an investigative process to respond to and document reports.

Your role

- Work in a safe manner, following your country's laws, regulations, and practices.
- Become familiar with, and follow, our safety and security programs and protocol.
- Immediately report safety or security issues or concerns, including threats or threatening behavior.

Immediately report safety and security issues or concerns, including threats or threatening behavior.

- In the U.S and Europe.: Call Enterprise Safety & Security 24/7 at +1.515.247.7233 (SAFE).
- Asia Pacific offices: Follow the established procedures for your location and notify the Pune Security Operations Center (PSOC) at +91-20-6906-6007.
- Latin American offices: Follow the established procedures for your location and notify Enterprise Safety & Security 24/7 at +1.515.247.7233 (SAFE).

I tripped on my way from the parking lot into work. I twisted my ankle, but I'm able to walk on it. A co-worker said I should report it. Why do I need to report it if I don't even think I need to go to a doctor?

Reporting incidents at work isn't only for major issues you might typically think of such as fires and bomb threats. It's also important to report things like falls, thefts, and on-the-job injuries—even if they seem minor. Reporting incidents provides documentation that is reviewed to identify and correct potential unsafe conditions

Site security

We provide risk-based physical controls and programs for all our offices globally. We check and document these controls on a periodic basis according to the risk level assigned to the location by Enterprise Safety & Security.

Your role

- Properly protect customer, company, and employee data.
- Keep your access control cards, keys, physical access codes, or other physical access instruments to yourself. If you stop working here, turn them in.
- Escort guests at all times.
- Work in a safe manner, following your country's laws and practices.
- Be familiar with, and follow, our safety and security programs and protocol.
- Physical security measures, protocol, and equipment are in place for a reason. Don't circumvent, disable, or destroy them.
- Immediately report to Enterprise Safety & Security if you:
  - Lose any access control cards, keys, physical access codes, or other physical access instruments (or if they're stolen).
  - See the circumvention, disabling, or destruction of physical security measures.
  - Have any safety and security issues or concerns, including threats or threatening behavior.

Emergency management

We have safety and security plans and protocols in place to address emergency situations. From fires, weather events, and health emergencies to any other threat or emergency, we've got you covered.

Your role

- Keep yourself familiar with our protocols for cooperating with, and complying with, the instructions of law enforcement, public safety, and security personnel. And be prepared to follow them.

In case of emergency, call 911 or the local public emergency services number for your location.

Enterprise Safety & Security can help if you need safety or security-related:

- Equipment
- Personnel
- Services
- Investigations
- Consulting

Business continuity

We uphold our commitment to our people and our customers by strengthening organizational resilience, identifying and protecting critical business functions, and developing actionable plans that ensure continuity of service during unexpected events.

Strong continuity planning helps us protect our people, data, and facilities as well as continuing to deliver consistent, reliable service to customers who depend on us. Principal maintains comprehensive policies and frameworks that include:

- Assessing risks and business impacts
- Maintaining incident management and emergency response processes
- Securing technology operations and disaster recovery capabilities
- Establishing clear communication plans for employees, customers, and partners
- Regularly testing and improving our continuity plans

Your role

- Know and follow emergency and continuity procedures relevant to your role, team, and location.
- Act promptly and responsibly during an incident, following direction from incident management, security, and technology teams.
- Report issues or potential risks that impact the ability to conduct business operations.
  - Use the Report an Incident page on Principal Passport.
  - Outside the U.S.: Follow the established procedures for your location.
- Participate in training, awareness activities, and exercises that strengthen our preparedness.

Brand and reputation management

The way we communicate our purpose, and every interaction with customers, employees, shareholders, business partners, and other stakeholders forms their opinion of us. We've earned success as a company known for our integrity and caring spirit by putting customers first and treating them fairly and ethically.

Having worked hard to establish Principal as a company people can count on to do the right thing, we are committed to ensuring our reputation, our brand, our good name, and our interactions make people proud to work with us.

Every employee is responsible for helping identify and report potential reputational risks. To learn more about scenarios or events that could cause negative publicity regarding our business practices, please refer to the Reputation Risk Management information for potential red flags.

We follow standards created to differentiate us, reinforce recognition, and help protect us and our customers from external threats. We monitor trends to proactively identify emerging issues before they become crises.

Highlighted topics:

› News media

› Social media

› Intellectual property

› Logo and trademark protection

› Brand expression standards

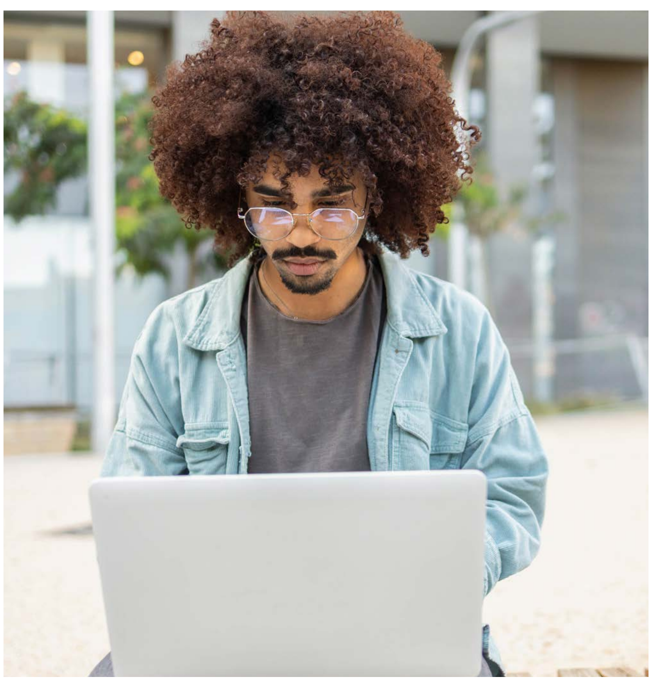
News media

We promote our company expertise and thought leadership through media outreach about new products, services and rankings, trends, and insights and research.

We proactively identify potential issues and manage our messages about those issues to the news media. Our Public Relations team is trained to handle requests from the public or other organizations for information about our company and the business we do.

Your role

- Refer any inquiry or question from the news media, security analysts, or our shareholders to the public relations team.
- If someone asks to interview you or wants you to speak on behalf of our company, check with the Public Relations team first. Interview requests from regulatory agencies are a different matter. See "Audits and outside exams."



Social media

Social media is a great way to connect with people and potential customers. We encourage our employees who participate in social media to do so in a respectful, relevant way that helps protect you, your co-workers, our customers, our reputation and, of course, follows the law and policies of your business area and location

Your role

When sharing on social media:

- Be respectful and professional to co-workers, customers, competitors, and others.
- Respect the privacy of others by confirming their permission before sharing photos that include them.
- Use caution on topics that may be considered objectionable or inflammatory.
- Respect all laws such as copyright, fair use, and financial disclosure laws.
- Feel free to like, comment, and share Principal posts with your own social network.
- Disclose your relationship when you post content about our products or services using #Principal_employee. Note: this guidance applies for U.S. social media and U.S. products and services. Outside of the U.S., consult your local legal or compliance contact for guidance as disclosure regulations vary by country.

FINRA/SEC rules impact the use of social media.

If you are a FINRA registered representative or an access person of a registered investment advisor, be sure to follow all applicable policies for using social media.

Intellectual property

We protect the ownership rights of our company and of others.

Your role

- Principal owns the copyright to any work of authorship (including computer software) created by you if:
  - the work is created as part of your job,
  - Principal pays you for the work, or
  - it was created in whole or in part using company facilities or equipment. This means everything - from emails you send, articles you write, reports you help create, or software you help design.
- If you're considering doing any work for a third-party using skills and equipment similar to those you use in your job, you need to get approval first, so be sure to talk with your leader.
- You must get written permission before using works copyrighted by others. This means you shouldn't use photos you've found off the internet or copy the written works of others.
- When designing materials with our logo, or the logo of a member company, make sure it conforms to the legally recognized mark format.
- Trade secrets are not to be shared outside the company and should only be shared internally with those who have a business need to know.

I am working on a PowerPoint presentation for a group of external advisors and customers. I have some slides from a presentation that I attended by one of our competitors and would like to include those slides in my presentation. I'll change a few words so that there isn't a copyright issue – this isn't a problem, right?

Yes, it is still a problem. It sounds like you are creating a "derivative work" of the competitor's slides, and the competitor can still assert copyright over derivative works. While using a small portion of another's work may constitute fair use, there is no clear test for when you are within this safe harbor. You should obtain permission from the content owner to use these slides.

Logo and trademark protection

Our brand, name, and logo are foundational parts of our reputation and must be protected as invaluable, strategic assets. Not only are they designed to identify and distinguish us in the marketplace, they represent Principal and what we stand for. Using our logo and trademarks correctly and consistently and making thoughtful decisions about who we allow to use our name and logo is important for protecting our Principal brand and preventing others from using them to mislead the public or damage our reputation as a company people can trust.

Your role

- Refer to our brand assets for guidance on how to use our logo and trademarks.
- Submit endorsement requests for review.
- Never modify logo color, form, or the relationship between name and symbol.
- Global locations must always use our Principal name and symbol together for trademark protection purposes
- Protect the trademark rights of the company and of others. Contact Global Brand & Experience (GBX) to ensure we're not infringing on others' trademarks when creating names for a new product or service.

Notify your leader and/or the Global Brand Management team if you notice improper use of our logo or trademarks.

Brand expression standards

Our brand expression standards outline how we present ourselves to the world – visually and verbally. They're intended to provide a balance of detail and flexibility needed to function across businesses, audiences, and geographic locations. Consistency protects our brand while helping build awareness.

When we speak and act as one Principal, we help people get to know us and how we can help them live their best lives. Remaining true to our Principal brand guides everything we do.

Your role

- Refer to our brand resources for tools and templates to modernize our communications, align with accessibility standards, and identify where and how to create consistent experiences.
- Our Brand Standards are not optional. They are to be followed as written.
- Work only with our designated Preferred Creative Partners to create print, digital, and video materials

Sustainability

At Principal, our purpose is to help more people, businesses, and communities gain access to financial security. Our sustainability strategy focuses on four thematic areas that directly support our purpose while creating value for society, the environment, and our business.

The four thematic areas include:

- Growing financial confidence for all
- Equipping small and medium businesses (SMBs) for success
- Investing for shared prosperity
- Fulfilling our people and teams

These focus areas enable us to integrate sustainability across the business and into our operations and decision-making. We share progress on our performance and outcomes in our sustainability reports, which are released annually. More information about our disclosures and Sustainability Reports can be found in the Data Center.

Highlighted topics:

› Our people and teams

› Customers

› Sustainable investing

› Environment

› Governance and business interactions

› Strengthening our communities

Start with the customer

Do what's right

Own what's next

Invest for our future

Our people and teams

We work to create and maintain a workplace where all employees thrive through a culture of inclusion, belonging, support, and comprehensive wellbeing.

Your role

- Be inclusive to all ideas and perspectives.
- If you're hiring, engage with our Talent Acquisition team or your local recruiter to learn how you can mitigate bias during the interview process.

Customers

We're committed to providing individuals and businesses with access to useful financial products, services, and education to meet their needs.

Your role

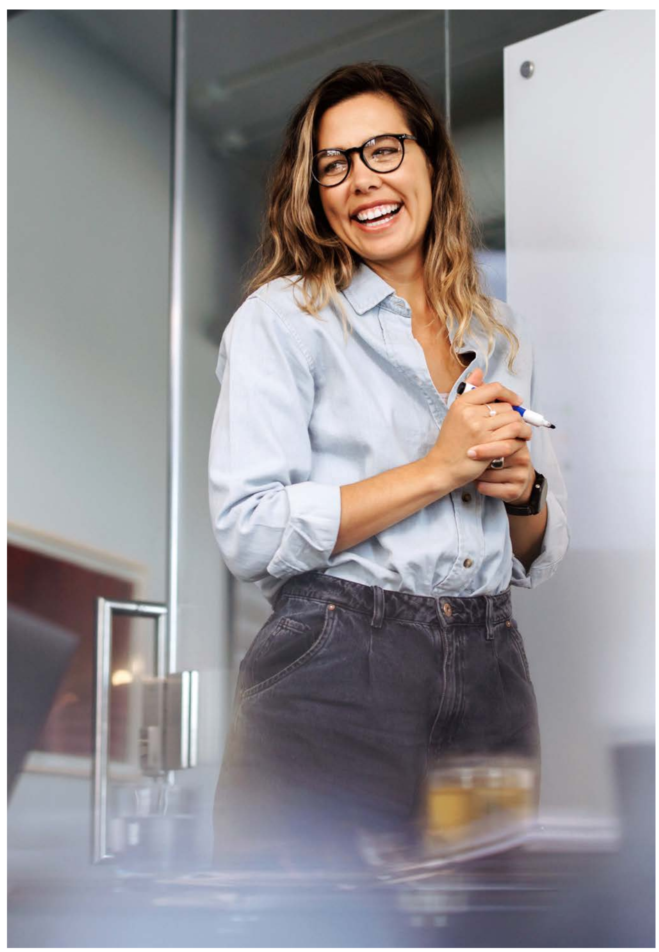
- If you're designing products or implementing new processes, keep accessibility and inclusion in mind.
- If you create customer materials or communications, use clear, simple language that's easy to understand and accessible to diverse audiences.
- If you're in a customer-facing role, ensure you understand the products and services you're discussing so you can provide accurate, helpful information.

Sustainable investing

Our sustainable investing beliefs are grounded in fostering relationships with investors and communities by offering products and solutions that align with their values. Our philosophy includes considerations of environmental, social and governance (ESG) integration and creating sustainable investment options that utilize a holistic view of factors influencing risk and return to help create added value for clients over time.

Your role

- Learn about ESG and sustainable investing at www.principalam.com.



Environment

We encourage environmentally responsible behaviors by our company, our employees, and our business partners. We have programs and initiatives to reduce our global greenhouse gas (GHG) emissions and increase energy efficiency, track our energy consumption, water usage, and waste production in the U.S., and engage our employees and third-party partners in supporting our environmental sustainability efforts.

Your role

- Turn off the lights when you're not using them.
- Use a reusable water bottle and coffee mug instead of plastic bottles and paper cups.
- Don't use Styrofoam food containers.
- Recycle your waste through the bins provided on campus.
- Engage with Green Team or local sustainability initiatives.

Governance and business interactions

Good governance is essential for any sustainable business and is especially important for financial service companies like ours, as our success is dependent on public trust. We consistently work to improve the effectiveness of governing policies, encourage ethical behavior, and promote transparency across our company. This means protecting customer and employee data, ensuring proper safeguards are in place, training all employees on Global Code of Conduct topics annually, and providing avenues for our stakeholders to raise any concerns.

Your role

- Protect customer privacy and confidentiality in all communications and transactions.
- If you're searching for a new supplier, focus on the procurement of goods and services from a variety of businesses that share our values of customer service, integrity, and quality, to ensure we can meet the varied and evolving needs of our customers.

To learn more about our sustainability efforts:

- Visit our Sustainability page on Principal Passport and at principal.com/sustainability.
- Read more about our ESG disclosures and reporting on our Data Center.
- You'll find details on the recognition we've received for workplace excellence, community involvement, environmental practices, and customer service in our current Company profile.

You can help further our sustainability strategy by keeping our corporate sustainability commitments top of mind as you work, and by letting us know how we're doing.

Strengthening our communities

Through volunteerism, philanthropic grants, and community-focused sponsorships and activations, Principal and Principal® Foundation strive to strengthen communities where we work and live around the world. For nearly four decades, Principal® Foundation has been supporting organizations that help eliminate barriers to a better financial future and expand access to essential resources and services, paving pathways to financial security and building stronger communities.

Specifically, our funding champions organizations working in three primary areas we consider foundational to moving people closer to the financial future they envision:

- Ensuring access to essential needs
- Fostering social and cultural connections
- Promoting financial inclusion

Resource Stewardship: In-Kind Contributions

We believe in the circular impact of our corporate resources. When corporate property—such as technology or office equipment—reaches the end of its internal life cycle, we seek to extend its value by supporting community-based organizations. To ensure security, equity, and compliance, all contributions of life-cycled corporate property must be processed through Community Relations. All in-kind requests must be made directly by a community organization through our portal.

Your role

- The Principal For Good program connects Principal employees to our philanthropic culture through volunteering opportunities and match giving programs that create lasting impact in our communities.
- Log into Benevity – where employees can make new donations, submit match giving requests, log volunteer hours, organize and manage volunteer events, request volunteer micro grants, sign up for local volunteer opportunities, and much more!
- Read more about our impact on principalfoundation.org

Glossary

Director: Members of the Board of Directors of Principal Financial Group, Inc.

Discrimination: Protected in U.S. Age, race, color, religion or religious creed, sex, gender, gender identity, gender expression, pregnancy, national origin, ancestry, citizenship status, mental or physical disability, medical condition, genetic information or characteristics, sexual orientation, marital status, domestic partner status, military status, protected veteran status, or any other characteristic protected by law.

Government Official:

- individual elected or appointed to a governmental entity regardless of rank,
- official or employee of a government,
- official or employee of a company wholly or partially owned or controlled by a government or a government entity. This includes state-owned entities such as sovereign wealth funds.,
- candidate for political office,
- political party or official of a political party, or
- person acting in an official capacity for any of the above regardless of rank or position.

Material information: Any information that a reasonable investor is substantially likely to consider important in making an investment decision. A few examples of material information include expected earnings for a given quarter, information about a potential merger or divestiture, revisions to financial statements, or changes in the board of directors, corporate officers, or our public accounting firm.

Money laundering: The movement of money from illegal sources or unlawful activities into legitimate businesses or activities.

Privacy incident: An occurrence that risks the security of personal data due to unintentional or unauthorized access, disclosure, destruction, loss, or alteration. Examples include:

- sending an email, fax, or letter with personal data to the wrong recipient.
- attaching and sending the wrong document in an email that contains personal data to someone.
- a programming error which results in someone seeing customer or employee personal data.

Worker: A current or former employee, director, in training non-employee, contingent worker, independent contractor, applicant/candidate/prospect, and non-employee financial professional.

Principal®

principal.com

Principal Life Insurance Company, Des Moines, Iowa 50392-0002.

EE11093-15 | 05/2026