

# Databricks Global Code of Conduct

## A Message from Ali Ghodsi

*Bricksters:*

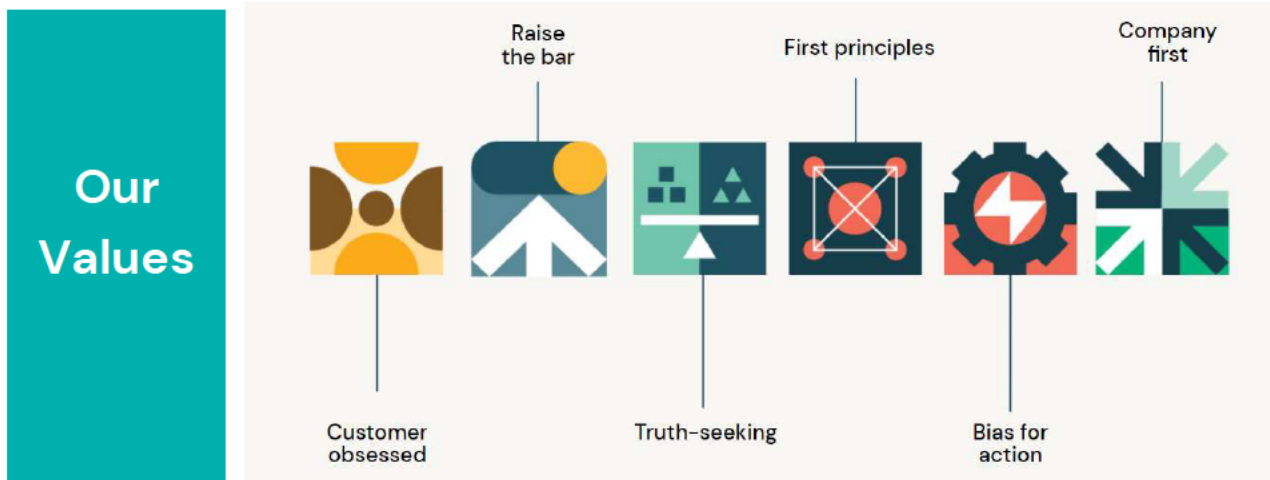
*Our Databricks values have always been central to everything we do. From how we interact with each other and our customers to how we innovate and collaborate as a global team, our core values are the roadmap for guiding our decisions. We are committed to building an inclusive, transparent, and ethical work environment where every Brickster feels welcome and supported.*

*I am happy to introduce our new Code of Conduct, which outlines key policies that ensure we are putting our values into action every day. The Code of Conduct sets guiding principles for our business and outlines the commitments we make to each other and our customers as Bricksters.*

*If you are ever unsure of how to handle a situation or are concerned about a violation, I want to encourage you to please speak up and reach out to your manager, the People team, or our Legal Compliance & Ethics team, or visit [go/speakup](https://go.databricks.com/speakup).*

*As Bricksters, we work with integrity, curiosity, and respect for each other. Thank you for your contributions as we continue to execute and scale, and ensure we authentically live our values along the way!*

ALI



# Contents

- Introduction & Important Reminders** ..... 4
  - The Code and Compliance & Ethics Behaviors..... 4
  - Conduct by Third Parties..... 5
- Speak Up & Investigations** ..... 5
  - Speaking Up & Non-Retaliation Policy ..... 5
  - Investigating Misconduct / Consequences of Violations ..... 6
- Ethical & Responsible Behavior** ..... 6
- Culture** ..... 7
  - Equal Opportunity Employment ..... 7
  - Diversity & Inclusion..... 7
  - Anti-Harassment and Discrimination ..... 8
  - Health & Safety..... 9
  - Substance-Free Environment Policy..... 9
  - Background Checks..... 9
  - Human Rights, Anti-Slavery and Human Trafficking ..... 10
- Trust**..... 10
  - Employee Privacy ..... 10
  - Confidential Information..... 11
  - Third Party Materials..... 12
  - Open Source ..... 13
  - Databricks Intellectual Property..... 13
  - Databricks' Equipment, Facilities and Resources ..... 14
  - Finance and Accounting Practices..... 14
  - Document and Data Retention/Management ..... 14
  - Legal Notice re: Employee Disclosures..... 15
- Integrity**..... 15

- Fairness and Integrity in All Business Dealings ..... 15
- Conflicts of Interest..... 16
- Fair Competition..... 18
- Global Trade Compliance, Export, and Sanctions..... 19
- Business Gifts, Meals, and Entertainment..... 19
- Internal Controls / Books and Records ..... 21
- Working with Governments** ..... 22
  - Working with Governments and the Public Sector..... 22
  - Who Is a Government Official? ..... 22
  - What Is in the Public Sector? ..... 23
  - Gifts, Expenditures and Gratuities to Government Officials: Anti-Bribery Policy..... 23
  - Organizational Conflicts of Interest ..... 24
  - Hiring Government Personnel..... 24
  - Sales to Government or Public Sector Customers ..... 25
  - Government Inquiries..... 25
  - Lobbying, Political Contributions and Volunteering ..... 25
- Communications**..... 26
  - Corporate Communications Policy..... 26
  - Brand..... 27
  - Social Media Policy ..... 27
  - Truthful Advertising and Marketing..... 28
- Partnerships & Contracting** ..... 28
  - Working with Third Parties ..... 28
  - Suppliers..... 29
  - Partner Program Vetting/Managing..... 29

## Introduction & Important Reminders

Our company's continued growth and success depend on everyone in the Databricks community acting responsibly and ethically every day. Behavior that breaks the law or appears improper – even if unintentional – could have serious financial or reputational consequences that could derail this exciting journey we are all on together.

### The Code and Compliance & Ethics Behaviors

This Code of Conduct (the “Code”) is the foundation of our legal Compliance & Ethics program. It defines what Databricks Inc. and its subsidiaries (collectively “Databricks” or the “Company”), expect from all employees, directors, officers, and board members (“You”). In short, **we expect everyone to model responsible, ethical conduct**, and specifically to:



#### Sample Behaviors

##### Play by the Rules

- Abide by our **policies**, complete required **trainings**, and model our **values** every day in internal customer, and business partner relationships
- Remember: [Go/policies](#)

##### Act with Integrity

- Know and follow the **Code**, conduct business **ethically**, letting our product speak for itself, and **model** our values to customers and partners
- Remember: [Go/ethics](#)

##### Speak Up

- Feel comfortable using our **Speak Up** program – a simple way to report misconduct – and know we **prohibit retaliation** for making good-faith reports
- Remember: [Go/speakup](#)

## Conduct by Third Parties

Databricks also expects partners, contractors, consultants, and others who may perform work or services for Databricks to follow the Code to the full extent it applies to their work with and on behalf of Databricks. We rely on everyone who manages these parties to communicate our expectations and have a zero-tolerance policy for unethical behavior. If You are concerned about any activity that violates this Code, including by a third party, You must Speak Up and raise those concerns.

Managers play a critical role in upholding Databricks' values and Code. Managers must lead by example, authentically live our values, hold themselves to the highest standards, and create an environment where others feel comfortable asking questions and raising issues. If someone on Your team raises an issue or asks a question, You as a manager must ensure the matter is handled correctly, including escalating appropriately through the relevant channels, which might include Legal Compliance & Ethics ("LC&E"), People, Finance or the Databricks' [Speak Up](#) line.

Several of the below areas are supported, or may be supported in the future, by other internal Databricks policies that provide more information. In addition to the links below, current versions are available at [go/policies](#). If You ever have a question whether a policy applies or how to interpret it, or **if You have questions about anything in this Code, seek help: contact Legal Compliance & Ethics ( [REDACTED] ) or Your People team representative.**

## Speak Up & Investigations

### Speaking Up & Non-Retaliation Policy

When it comes to identifying misconduct, You, our employees, are our best asset, and we expect You to stay vigilant. To that end, You must report suspected or actual violations of laws, rules, regulations, or this Code immediately upon learning of the issue. Throughout the Code, there are suggestions where to escalate certain matters, but You may always contact People ( [REDACTED] ) or LC&E ( [REDACTED] ) for assistance. Relatedly, if You have any questions about this Code or any referenced policy, including if You are unsure whether a violation has occurred, contact LC&E or People.



Databricks will not tolerate retaliation against anyone who reports a good-faith concern of a violation or suspected violation, or against anyone who assists in an investigation of a reported violation. Please immediately report to People or LC&E any acts that appear to be retaliatory.

Important: If You prefer to remain anonymous, You can report concerns anonymously to Databricks' [Speak Up](#) line, except where anonymous reporting might be restricted by local law. Especially if You choose to report anonymously, please provide as much detail as possible about the concern so that Databricks can properly investigate.

### Investigating Misconduct / Consequences of Violations

A violation of this Code – or the law – is serious. Databricks will thoroughly and fairly investigate all good-faith reports. If asked, You are expected to cooperate fully with our investigations. Any information You provide will be kept confidential to the extent possible. If You have questions about our investigation procedures, including what you can expect in an investigation, check our [go/ethics](#) site for more information/FAQs.

Anyone found to have violated the Code will be subject to appropriate disciplinary action, which can range from additional training and coaching up to and including termination of employment.

## Ethical & Responsible Behavior

Our Code is divided into the following sections, which describe the various behaviors we expect You (and our third parties, as relevant) to own:

Building and maintaining a fair, safe, and inclusive **Culture** at Databricks

The mutual **Trust** needed among Databricks, our employees, customers, and others when it comes to handling information, data, and assets

The **Integrity** required in business dealings to avoid legal, financial, and reputational harm

Some special rules for **Working with the Government**

Ensuring **Communications** about Databricks are appropriate and properly vetted

What we expect of Databricks **third parties**, including Partners and suppliers

## Culture

### Equal Opportunity Employment

Databricks is an equal opportunity employer. We do not discriminate on the basis of race, religious creed (including religious dress and grooming practices), color, sex or gender (which includes pregnancy, childbirth, or related medical conditions), gender identity, gender expression, age, national origin, ancestry, citizenship, political activity or affiliation, sexual orientation, physical or mental disability (including AIDS and HIV status), medical condition (including cancer, genetic characteristics and as otherwise defined under applicable law), veteran or military status, marital status, taking or requesting statutorily protected leave, or any other basis protected by federal, state or local law. All such discrimination is unlawful.

In addition, Databricks prohibits the harassment of any individual on any of the bases listed above or any other characteristics protected by law. This policy applies to all employment decisions and conditions of employment, including hiring, placement, promotion, performance review, training, transfer, facilities, compensation, benefits, programs, and terminations. Consult our [Discrimination, Harassment & Retaliation Prevention Policy](#) for more information.

### Diversity & Inclusion

Databricks is committed to fostering, promoting, cultivating, and supporting a culture of diversity, equity, and inclusion. We recognize that the collective sum of the individual differences, life experiences, knowledge, inventiveness, innovation, self-expression, unique capabilities, and talent that our employees invest in their work represents a significant part of our culture, reputation, and brand. We embrace and encourage our employees' differences in age, color, disability, ethnicity, family or marital status, gender identity or expression, language, national origin, physical and mental ability, political affiliation, race, religion, sexual orientation, socio-economic status, veteran status, and other characteristics that make our employees unique.

All employees at Databricks have a responsibility to always treat others with dignity and respect. All employees are expected to exhibit conduct that reflects inclusion during work, at work functions on or off the worksite, and at all other company-sponsored and participative events. All employees are also required to complete

unconscious bias training during employee onboarding.

Any employee found to have exhibited any inappropriate conduct or behavior against others may be subject to disciplinary action.

Employees who believe they have been subjected to any kind of discrimination that conflicts with the company's diversity policy and initiatives should seek assistance from a manager, senior manager, or member of the People team.

## Anti-Harassment and Discrimination

Databricks is committed to maintaining a respectful, non-retaliatory workplace environment that is free of harassment, intimidation, bias, and unlawful discrimination of any kind. Harassment and any conduct that may foster an intimidating, offensive, or hostile work environment, including unwelcome or unsolicited sexual advances, threats of physical harm, or violent behavior, or use of discriminatory slurs or inappropriate remarks or jokes, are strictly prohibited. Databricks has a zero-tolerance policy for violence and threatening behavior, including verbal or physical conduct or communications involving a legally protected category that are unwelcome or interfere with an employee's work performance.

This policy applies to all work-related settings and activities, whether inside or outside Databricks' offices, and includes business trips and work-related social events. All employees and contractors are responsible for abiding by and helping to enforce this policy by reporting any behavior they believe does or may violate this policy. Reports can be made to an employee's or contractor's manager, senior manager, a member of the People team, or the Chief People Officer. Any manager who receives a complaint of unlawful harassment must report it immediately to the People team. Employees and contractors will never be penalized for speaking up to report a possible violation of Databricks' policies or for cooperating with an investigation. On the other hand, knowingly making false or malicious reports will not be tolerated, and anyone filing such reports will be subject to appropriate disciplinary action up to and including termination. Consult our [Discrimination, Harassment & Retaliation Prevention Policy](#) and [Health & Safety Policy](#) for more information.



## Health & Safety

Databricks is committed to providing a healthy and safe work environment. Health and safety are shared responsibilities, and all employees, contractors, consultants and visitors must comply with health and safety laws and Databricks policies, and promptly report accidents, injuries, and unsafe equipment, practices, or conditions to our People ( ) or facilities ( ) teams.

Databricks does not tolerate threats, threatening behavior (including intimidation, bullying, physical or mental abuse, coercion, or stalking) or acts of or implied violence by anyone. Databricks also strictly prohibits employees, or any other person providing services to Databricks or located on the company's premises, from possessing weapons of any kind at the workplace.

Consult our [Health & Safety Policy](#) for more information.

## Substance-Free Environment Policy

Employees are prohibited from possessing, using, or being under the influence of alcohol or recreational drugs while on the job (with the exception of the use of alcohol at authorized company events as noted below). Distribution, dispensation, manufacture, possession, sale, purchase, or use of an illegal or recreational drug or controlled substance while engaged in Databricks business is also strictly prohibited.

Alcohol may be available in some Databricks offices, provided at company events, or purchased while entertaining customers or partners as representatives of the company. However, You are expected to use good judgment and not drink in a way that leads to impaired performance or inappropriate behavior, puts yourself or others in danger, or violates the law. Employees are strictly prohibited from driving a vehicle while on Databricks' business (including transporting other employees to and from an event) while under the influence of alcohol or any other substance that could result in illegal driving under the influence.

As a condition of employment, Databricks employees must abide by the terms of the [Illegal Drugs & Controlled Substances](#) Policy.

## Background Checks

Databricks is proud to have a highly skilled and professional workforce that provides first class solutions for our customers. To ensure Databricks continues to hire and

retain the best talent, stays consistent with industry best practices, and ensures compliance with commitments to our customers, Databricks requires all employees and specific categories of contractors to undergo a background check. Databricks complies with all applicable laws relating to background checks, including any prohibitions or restrictions on certain types of background checks in the countries where we operate. Consult our [Background Check Policy](#) for more information.

### Human Rights, Anti-Slavery and Human Trafficking

Databricks supports and respects the protection of internationally recognized human rights and labor standards. We are committed to upholding the fundamental human rights of our fellow employees, and other individuals in our global network, and we expect the same of our partners, vendors and others who provide services on behalf of Databricks. We don't engage in and do not condone child labor, forced, bonded, or indentured labor, involuntary prison labor, slavery, trafficking of persons, commercial sex acts, or physical punishment – and we comply with all U.S. and non-U.S. laws covering these topics. We pay applicable legal wages under humane conditions and expect our partners and vendors to do the same.

Consult our [Anti-Slavery & Human Trafficking Policy](#) for more information.

## Trust

### Employee Privacy

Data and information are powerful tools, and Databricks is committed to protecting them, especially when they include personal information about our employees. We will always endeavor to collect only personal information relevant to the employment relationship and our business activities, use any such information only in an appropriate way, consistent with legitimate business needs and legal requirements, and maintain reasonable safeguards to protect Your personal information. Consult our [Global Privacy Notice for Personnel](#) for more information.

## Confidential Information

It is critical that we protect all confidential and proprietary information of and about Databricks, as this information is one of our most valuable assets. We must also protect confidential information that other parties have shared with us, including any that we receive from our customers. Even if information is not marked “confidential,” any material whose contents are confidential in nature must be treated as confidential.

Confidential information refers to non-public information. Here are some examples:

- Financial information and projections, such as sales bookings or sales pipelines;
- Source code and technical information;
- Product plans and roadmaps;
- Business strategies such as plans for an acquisition, financing transactions or management changes;
- Personal information of or about individuals, including other employees; and
- Non-public information of or about customers, partners, investors or other third parties.

### Databricks Confidential Information

In Your work at Databricks, You will be exposed to and learn confidential information about the company. As a rule, Databricks’ confidential information should not be disclosed externally without a Non-Disclosure Agreement (NDA) in place. This means You should not share Databricks’ confidential information with any outsiders, including Your family or friends, or take any action, including trading, based on Databricks non-public information in violation of our [Insider Trading Policy](#).

You must also limit sharing of Databricks’ confidential information internally. Confidential information should only be shared with others at Databricks who have a need to know the information to perform their job. For more information about handling Databricks’ confidential information and data classification standards, please see Databricks’ [Security, Privacy and Data Protection Policies](#).

### Third-Party Confidential Information

Databricks (and You) may also be entrusted with confidential information of third parties: from customers, prospects, partners, investors, or job applicants. This information must also be handled carefully and appropriately.

When You do have permission to use another party's confidential information, make sure to:

- Comply with any contractual obligations like those in an NDA or other confidentiality obligations, which may include return or destruction obligations;
- Use the information only for its intended purpose;
- If sharing internally within Databricks, only share the information with others who need to know it to perform their job;
- Transmit the information securely;
- Never trade in the stock of any company based on non-public information You learn about that company; this is a violation of this Code of Conduct, our [Insider Trading Policy](#), and the law; and
- Always follow Databricks' [Security, Privacy and Data Protection Policies](#).

You may only take, accept, or use third-party confidential information if You have official permission. Casual acceptance or use of confidential information creates risk that Databricks will be accused of misusing it (see the Fair Competition section below).

If You have or receive confidential information that You should not have, do not use it, access it, or delete it, and immediately contact Legal ( [REDACTED] ).

### Third Party Materials

The successful operation of our business requires many interactions with third parties, usually entities providing a product or service we need in order to provide Databricks services. However, unsanctioned software or services may present a significant risk to Databricks. All third-party software, services, or products require a [security assessment](#) to verify that they meet our security requirements, as set forth in our [Security, Privacy and Data Protection Policies](#) and in appropriate licensing or subscription documentation. Our Procurement team ( [REDACTED] ) can help ensure these processes are followed and requirements are satisfied.

Where Databricks does utilize third-party materials, it is also important that we respect the third party's intellectual property, including rights protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations.

Unauthorized use or copying of third-party materials could expose Databricks or You to civil and criminal liability. For more information, please see the Acceptable Use

Policy in Databricks' [Security, Privacy and Data Protection Policies](#).

## Open Source

At Databricks, we believe in open source. Consistent with Databricks' policy of respecting the valid intellectual property rights of others, Databricks complies with the license requirements under open-source software licenses. You should always follow the Open Source Policy, located in our [Security, Privacy and Data Protection Policies](#). If You have any questions about open source, consult with Legal ( [REDACTED] ).

## Databricks Intellectual Property

Intellectual property is Databricks' most valuable corporate asset, and everyone on the team contributes to creating, marketing, and protecting it. Intellectual property includes many things, such as: patents, trademarks, copyrights, trade secrets, source and object code, marketing plans, training materials, know-how, and other confidential and proprietary information. It is of the utmost importance that we protect Databricks' intellectual property and the competitive advantage it provides. Unauthorized use can lead to the loss of value and could be devastating to the business.

Your employment agreement with Databricks has important intellectual property ownership and assignment provisions in it - please make sure to review it if You have questions. When You create new intellectual property in the course of Your employment with Databricks or using Databricks' resources, please immediately notify Your manager so that the Company can make a determination as to whether to seek formal protections.

Any third-party use of Databricks' intellectual property, including Databricks' trademarks and logos, must be approved in advance by Marketing or Legal. You should report any misuse or suspected misuse of any Databricks' intellectual property immediately to Legal ( [REDACTED] ). Likewise, Databricks expects You to respect the intellectual property of others. Inappropriate or unauthorized use of another party's intellectual property may expose You or Databricks to civil or criminal liability. Please consult with Legal before accepting or using proprietary information from others.

## Databricks' Equipment, Facilities and Resources

Databricks provides equipment, technology, systems, facilities, and other resources (collectively "Databricks Resources") to You so that You can perform Your work. Databricks Resources are the property of Databricks and, to the extent permitted by law, Databricks may monitor and access Databricks Resources, with or without Your knowledge or approval.

Databricks Resources should be used primarily for business purposes. However, minimal incidental personal use is permitted.

For more information about appropriate use of Databricks Resources please review the Acceptable Use Policy in [Databricks' Security, Privacy and Data Protection Policies](#). If You have any questions or need to report misuse of any Databricks Resources, immediately contact Security ([REDACTED]).

## Finance and Accounting Practices

Databricks engages in finance and accounting-related practices consistent with generally accepted accounting principles and relevant obligations for our Company. You must support these practices and never seek to subvert or evade them, or to mislead or provide inaccurate information to any of our finance or accounting resources in the course of our accounting and review procedures. If You have questions at any time about relevant requirements, contact the Finance team.

## Document and Data Retention/Management

We may be required to retain certain business records for specific periods of time, and there are certain situations, such as in the context of litigation, investigations, or audits, where You may be asked to retain records. You are expected to comply with any guidance issued by our Legal, People, Security, or other teams in this regard.

In addition, for current guidance on appropriate data (personal/customer data) retention practices, consult the Data Retention Policy within our [Security, Privacy and Data Protection Policies](#).

## Legal Notice re: Employee Disclosures

Databricks wants to ensure You are aware that, notwithstanding this Code of Conduct or any other Databricks policy, You are not prohibited or limited from filing a charge or complaint with, or otherwise communicating with or participating in any investigation or proceeding conducted by, any federal, state, or local government agency or commission (“Government Agencies”) and may do so without giving notice to or getting permission from Databricks (a “Government Communication”). You are also not prohibited from disclosing documents or other information pertaining to Databricks to Government Agencies in the course of a Government Communication. You should, however, take all reasonable precautions to prevent unauthorized use or disclosure of Databricks’ confidential information to any party other than a Government Agency. You are also not permitted to disclose any material that is subject to Databricks’ attorney–client privilege or that is attorney work product.

Furthermore, pursuant to 18 U.S.C. Section 1833(b), You will not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that: (1) is made in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney, and solely for the purpose of reporting or investigating a suspected violation of law; or (2) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

## Integrity

### Fairness and Integrity in All Business Dealings

Databricks has a responsibility to our customers, investors, and the marketplace to behave transparently and fairly and follow the highest standards of ethical business conduct. Accordingly, we expect each and every Brickster to Act with Integrity at all times. It is a violation of this Code to engage in unethical business conduct, including any behavior that could affect Your ability to be fair and impartial, such as:

- Accepting a bribe, kickback, or improper gift or rebate from a vendor/supplier;
- Having a significant, undisclosed conflict of interest/outside activity that could harm Databricks (see Conflicts of Interest below); or

- Engaging in fraud, money laundering or any illegal scheme, whether alone or in collusion with someone else.

It is also a violation of this Code to engage in any behavior that breaches the integrity of our business or the marketplace, such as:

- Paying bribes, whether to customers or anyone else who exercises discretion on business matters (see Working with Governments – Improper Payments below);
- Engaging in anti-competitive conduct, such as improper bid coordination, improper use of confidential or non-public information, price fixing, or any other conduct that violates fair competition laws;
- Working with any third parties that we are prohibited from doing business with under relevant sanctions or export control regimes, or where the relationship itself could otherwise expose us to other serious legal risks;
- Falsifying or altering any company books or business records so as not to fairly or accurately record the terms of a transaction or otherwise hide the truth in any way; or
- Evading or subverting any required Databricks or third-party business processes or controls.

## Conflicts of Interest

### Conflicts of Interest Defined

Part of ensuring fairness and transparency is avoiding activities or relationships where your personal interests and our company's interest could conflict, or appear to conflict, due to a personal relationship, outside employment or investments, or other situations. Conflicts can arise when you, for example:

- Engage in any activity that competes with the Company
- Let your business decisions (including job-related decisions) be, or appear to be, influenced by family interests or personal financial interests
- Use company assets, relationships, or data to promote a personal interest (e.g., a side business or role)
- Have outside activities or employment that negatively affect your job performance or interfere with your duties to Databricks



- Work for, provide services to, have a financial interest in, or receive any personal benefit from a current or potential vendor, customer, or competitor – or have a close family member who does.

### Disclosure and Clearance of Conflicts

Simply having a conflict of interest is usually not a policy violation, but failing to disclose it promptly is. You must disclose actual or potential conflicts for review ahead of time using the form at [go/disclose](#). LC&E will review your disclosure and either clear the conflict or request additional information or in some cases may have to reject the activity. Employees may not proceed until they receive clearance from LC&E.

Databricks understands that employees may have other outside activities (e.g., volunteer work, advisory boards, etc.) that do not conflict with Databricks' interests. Databricks employees can engage in these activities, as long as they will not impact or interfere with job performance or responsibilities or use company data and other resources other than as allowed under our Acceptable Use Policy. Managers can find guidance on identifying and evaluating potential conflicts at [go/manager](#).

### Disclosure Requirements: Examples

Below are examples of items that do and don't require disclosure. If you are unsure, you should err on the side of disclosing, or contact LC&E with questions.

#### Do Disclose

1. Significant financial interests you or a close family member has in a Databricks vendor, partner, customer, or competitor (excludes nominal equity ownership, i.e., of <5% of any company or 1% of public companies)
2. Advisor, board, or other business roles for Databricks vendors, partners, customers, or competitors, or personal receipt of fees from any of these parties
3. A close family relationship with (1) another Databricks employee in your management chain or immediate team; or (2) a vendor, partner, customer, prospect or competitor
4. A side business that directly competes with Databricks or has overlapping customer or partner bases

### Don't Disclose

1. Outside activities that will not interfere with your Databricks role or take place during business hours
2. Public speaking engagements, which instead should follow the rules in our [Brickster Communications Guidelines](#) (e.g., Comms review).
3. Nominal equity or stock ownership (<1%) in any company

### **Fair Competition**

Databricks is committed to outperforming any of our competition fairly and legally. We Play by the Rules, including laws governing antitrust and fair competition, and avoid behaviors that could cause risk of violations, including:

- Unlawfully discussing prices, costs, customers, sales, or markets with competitors or their employees;
- Making any unlawful price-setting agreement or agreements with competitors – formal or informal – to fix other terms of sale, coordinate bidding activities, or allocate customers or territories;
- Improperly using or disclosing to the Company any proprietary information or trade secrets of any former or concurrent employer or other person or entity;
- Improperly using or authorizing the use of any inventions that are the subject of patent claims of any other person or entity;
- Making untruthful or unfair statements about competitors' products or services; or
- Any other conduct that could be seen as discouraging competition or as an unfair market practice.

You should never talk about any matters relating to our competitive position – including Databricks or competitor information or practices – with our competitors, even in informal settings like conferences. Limited benchmarking discussions can be appropriate with guidance from Legal. If You anticipate these discussions, contact [REDACTED] as far in advance as possible.

Finally, any business – or personal – social media or other external communications that may reference competitor products or services must always comply with our [Brickster Communications Guidelines](#).

## Global Trade Compliance, Export, and Sanctions

Databricks complies with applicable global trade laws, including import and export laws, sanctions, and anti-boycott rules and regulations. Global trade laws control both where Databricks may send or receive its products and services and to whom Databricks may sell its products and services. These laws are complex and apply to:

- Imports into and exports from the U.S.;
- Imports into and exports from other countries where those products contain technology or components with origins in the U.S.;
- Exports of services to non-U.S. persons; and
- Exports of technical data, in particular if that technical data originates in the U.S.

The following examples may constitute an export or an import:

- Exposing or allowing access by non-U.S. nationals to U.S. technical data, regardless of where the exposure occurs;
- Permitting software to be downloaded or used in a different country; and
- Transporting technical data or software on a device (such as a laptop or phone) in luggage while traveling to another country.

Databricks is prohibited from procuring goods or services from and selling goods or services to any individuals or entities subject to a trade embargo. Currently, embargoes apply to individuals and entities in or controlled by Cuba, Iran, North Korea, Syria and the Crimea, Donetsk, and Luhansk regions of Ukraine. Our business transactions may also be subject to other government-imposed sanctions or boycotts that could restrict our ability to do business with certain entities and individuals or which may require other legal protections to ensure our product is not used by bad actors for the wrong purposes.

Contact LC&E ( [REDACTED] ) immediately if You learn of any situation that could appear to involve embargoed or sanctioned territories, entities, or individuals, or where our product may be being used for an improper purpose.

## Gifts and Entertainment

Company resources are to be spent responsibly. Although gifts, meals, travel, and entertainment may be legitimate business expenses, they should never be used to

improperly influence a third party, whether a customer, a supplier, a government official, or anyone else. The reverse is also true: You should never be influenced by a gift or any other value and should always refuse any gifts that are inappropriate or against our policies – unless it would be offensive in the moment (e.g., for cultural reasons) to do so. In these cases, contact LC&E for guidance what to do with the gift.

Giving or receiving gifts, meals, travel, and entertainment that are extravagant or lack a legitimate business purpose can expose the company to legal or reputational risk, as they may be considered bribes or create an appearance of impropriety.

### Gifts and Entertainment Guidelines

A business gift (including paying for a meal or travel) or entertainment is generally acceptable only if **all** the following are true:

- The counterparty is not a vendor/supplier (i.e., You should generally avoid gift-giving or receiving with vendors/suppliers, unless it is a nominal gift like low-value company-branded swag or a deal-gift, or a drink/cup of coffee incidental to a business meeting);
- It is not a cash gift (or cash equivalent like a prepaid debit card);
- It is not extravagant or excessive in value (and generally under \$75, unless even that amount would appear excessive in Your location);
- It is not provided frequently;
- It is not one of multiple small gifts that, in conjunction with others, can be construed as a larger, expensive gift;
- It is consistent with customary business practices;
- It complies with applicable laws and regulations (including U.S. Foreign Corrupt Practices Act and the UK Bribery Act – see Working with Government Officials below) and our [Global Anti-Bribery & Anti-Corruption Policy](#);
- It will not place the recipient under any obligation to the gift-giver;
- It is not being provided during or close in time to a bid, contract negotiation, or renewal, license or permit application, or other pending business matter;
- It cannot be construed as a bribe, kickback, or payoff; and
- If You are giving or paying for a gift, the gift also complies with Databricks' [Global Expense Policy](#).

Here are a few examples of gifts that are normally acceptable:

- Company swag (promotional items with Databricks' brand or logo);

- Meals and entertainment of reasonable value during which business (which may include appropriate, professional client development) is being conducted;
- Prizes randomly received at industry conferences or in raffles or contests;
- Small gifts of minimal value that are customary on certain holidays or for certain occasions such as weddings or births.

If You have questions or concerns about whether gifts and entertainment are appropriate, always reach out to LC&E ( [REDACTED] ). You must also notify LC&E if You receive or would like to receive a gift that is excessive or unusual or does not comply with the above guidelines, which should only be done on an exceptional basis.

Important: Violating these rules when giving gifts to government officials can expose us to significant legal risk. Accordingly, all gifts and other things of value to be provided to the government must be reviewed ahead of time (i.e., before giving them) with LC&E using our [Value to Government Officials Disclosure Form](#), also available on [go/ethics](#). Review the Working with Governments – Improper Payments to Government Officials section below and, for more information, consult our [Global Anti-Bribery & Anti-Corruption Policy](#) and the FAQs section of [go/ethics](#).

## Internal Controls / Books and Records

To operate a successful business and mitigate important risks, Databricks has built internal business processes and controls. These are important and intentionally designed to comply with relevant laws or obligations, and You must follow them. Depending on the situation, failing to play by our rules can be a serious violation of this Code or worse, might be illegal. For clarity, intentionally evading or undermining, or failing to cooperate in a company process, including an audit or investigation (or another important process, like a customer's business processes for suppliers) is always a violation of this Code that could result in discipline.

Databricks also maintains company books and records that fairly and accurately represent our business activities and transactions. You must do so as well. Failing to keep accurate records can also allow misconduct that harms our company to go undetected, so please be vigilant. This applies to everything from financial books, statements, and accounts to more routine business records and communications like our customer files and business communications, including emails and instant

messages (e.g., Slack). Therefore:

1. Never intentionally alter or falsify a company record, or record a payment as being for a purpose other than its true purpose (e.g., recording an improper payment as a consulting fee or marketing expenses);
2. Transactions should never be made without proper authorizations and should be recorded transparently to allow for the preparation of accurate financial statements;
3. Never establish any undisclosed, unrecorded or “off-the-books” account or “slush fund,” including an account held by a third party for our benefit;
4. Always comply with any record-keeping requirements set by Your team and Databricks; and
5. Never write any business-related messages in any form (emails, Slack, etc.) that mischaracterize or conceal the truth of the matters they discuss.

## Working with Governments

### Working with Governments and the Public Sector

Special rules apply to our business and other dealings with governments or public sector organizations of any kind – U.S. (federal, state, or local) or foreign, including government-owned or run entities like universities and hospitals, telecommunications services, and even some financial institutions. It doesn't matter where You are located or which Databricks entity You work for: You are responsible for understanding and complying with this section and all applicable requirements in the U.S. or any other country. A violation of this policy or of applicable laws can lead not only to serious financial and reputational harm but also to Databricks being prohibited from doing business with governments.

### Who Is a Government Official?

A government official is any elected official, royal family member, or any person who works for or is an agent of a government (at the national, multi-national, state or local level), a government-owned, or a government- or state-controlled entity. Remember: this might include employees or agents of state-run universities and hospitals,

telecommunications services, and even some financial institutions. Government officials can also include employees of public international organizations like the United Nations or World Bank, political party officials or candidates for office. If You have any questions whether You are interacting with government official, reach out to LC&E, and consult our [Global Anti-Bribery & Anti-Corruption Policy](#) for more information.

### **What Is in the Public Sector?**

The Public Sector includes any party (including a customer) who is under public or quasi-public (not private) control, whether actual or effective control, and includes government and quasi-government parties such as government owned or run medical or academic institutions, law enforcement, and certain utility companies. For additional information, consult the FAQs section of our [go/ethics](#) site.

### **Gifts, Expenditures and Gratuities to Government Officials: Anti-Bribery Policy**

Many countries have strict laws prohibiting bribing, giving, offering, or promising anything of value to government officials where the goal is to improperly influence them to gain a business advantage. These laws include the U.S. Foreign Corrupt Practices Act (“FCPA”) and the UK Bribery Act, as well as similar laws in other countries.

These laws not only ban bribery, improper payments, gifts, and gratuities, but also prohibit giving – or even offering or promising – any value including, for example, meals and entertainment, political or charitable contributions or donations, equipment, job offers (including jobs for friends or family of a government official), inside information, volunteer time, or improper discounts or rebates. In addition, these laws apply whether the gifts, expenditures and gratuities are given by Databricks employees or through third parties, such as lobbyists, agents, consultants, suppliers, or service providers, or through political action committees (PACs) or similar methods.

Certain laws may also limit the amount or frequency with which individual government officials or entities can accept gifts or hospitality. To this end, LC&E may have visibility into prior gifts, expenditures, or gratuities given to government officials, including within the same government entities, of which You are unaware. Seek review from LC&E using our [Value to Government Officials Disclosure Form](#), also available on [go/ethics](#), before giving anything of value (including the items mentioned above) to any government officials to be sure You understand the rules of engagement and to let Databricks have

a chance to mitigate any risks.

For more information, consult the Conflicts of Interest and Gifts and Entertainment sections above, and Databricks' [Global Anti-Bribery & Anti-Corruption Policy](#).

## Organizational Conflicts of Interest

Many countries have strict laws prohibiting company or organization-specific conflicts of interest known as Organizational Conflicts of Interests (OCIs). In the U.S., the Federal Acquisition Regulations (FAR) define OCIs as situations where, because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

As relevant for Databricks, OCIs occur when a government contractor's work on a government contract appears to compromise its ability to work on or compete fairly on another government contract. Examples of OCIs include when information received during work for a government entity provides a competitive advantage for a new government contract, or when a prior government contract involves setting ground rules for a new contract or evaluating a competitor. Non-disclosure of an OCI can lead to serious consequences to Databricks, so please be sure to contact the Public Sector Legal team ( [REDACTED] ) if You know or suspect an OCI may exist.

## Hiring Government Personnel

Special laws apply to hiring current and former government personnel, and there are notification requirements associated with Databricks' performance of work for a government entity that might lead to a conflict of interest. There are limits on who Databricks may recruit or hire based on the prospective employee's current or prior roles working for government institutions. For example, Databricks may not be able to hire someone whose prior responsibilities included assessing or making purchases of Databricks' offerings on behalf of a government entity because it could appear that an offer for employment was in exchange for favorable behavior while working as a government employee. Government employees may also be required to obtain specific approval from the government or an ethics opinion prior to working at Databricks. Contact the Public Sector Legal team ( [REDACTED] ) or



People before offering employment to a current or former government employee.

### **Sales to Government or Public Sector Customers**

When a government or public sector organization is our ultimate customer, we are often subject to stricter requirements compared to when we work with private sector customers. If Your work involves interacting with or selling to a government or public sector entity, You are responsible for knowing and complying with all applicable requirements. These requirements can be complex, and a violation can lead not only to serious financial and reputational harm but also to Databricks being prohibited from doing business with the governmental entity. You must avoid improperly soliciting or obtaining confidential information, such as sealed competitors' bids, from government officials prior to the award of a contract. Contact Legal ( [REDACTED] [REDACTED] ) with any questions about working with Public Sector customers.

### **Government Inquiries**

Immediately refer all government-directed subpoenas, requests for documents, interviews, or other information, and any other government inquiries to Legal ( [REDACTED] [REDACTED] ). These requests may come from law enforcement, regulatory agencies, inspectors general, or similar entities or officials. If You are unsure whether the request is from a government entity, please contact Legal for guidance. Legal will work with You to ensure all responses are appropriate and avoid disclosure of trade secrets, confidential information, or privileged information or materials.

### **Lobbying, Political Contributions and Volunteering**

From time to time and when determined to be in the best interest of the company, Databricks may engage in discussions with various levels of governments to express opinions and perspectives regarding public policy issues of interest to the Company. Various laws govern these discussions, whether performed by certified lobbyists, trade associations, or otherwise. Employees must comply with these laws and notify their manager and Legal ( [REDACTED] [REDACTED] ) ahead of engaging in discussions, including if You want to investigate or use lobbying activities or lobbyists on behalf of the Company. Note that LC&E may advise the conduct of specialized due diligence

before using types of actors.

Additionally, from time to time and when determined to be in the best interest of the company, Databricks may contribute to PACs, organizations, or candidates for office if their causes align with Databricks' business. Various laws govern these contributions. Employees must comply with these laws and notify their manager and Legal when engaging in discussions about possible contributions.

Databricks employees have the right to participate in the political process by making personal contributions from personal funds, subject to applicable legal limits and requirements. Databricks will not reimburse You for any contributions. Please contact Legal with any questions regarding this policy.

Employees are encouraged to participate in the community and the political process; however, employees may not create the impression that their activities are supported by, or are performed on behalf of, Databricks. Employees may voluntarily participate in campaign activities but must do so on their own time, utilizing Databricks Voluntary Time Off (VTO) Program, or by taking paid time off or an unpaid leave of absence. In situations where Databricks employees wish to enter public service, they must do so clearly expressing that their actions do not represent Databricks.

Be sure to let Legal and Your manager know if You work or volunteer with a government entity to be sure that Databricks complies with the law, and to enable the company to take appropriate measures to ensure no conflicts of interest exist. Consult the Conflicts of Interest section above for more information.

## Communications

### Corporate Communications Policy

Databricks employees may not speak on behalf of Databricks unless they are part of Databricks' Public Relations or Investor Relations team or have been specifically authorized to make a statement by the Public Relations or Legal team.

Information about Databricks, its products, and its financial results or projections, or information about current or former Databricks employees, directors, or customers, is considered confidential and may not be shared or discussed outside of Databricks. In the event outside sources like the press, investors, or analysts reach out to You

requesting such information, You must decline to comment and immediately contact [REDACTED].

Before posting opinions or information about Databricks on the internet (including social media, user forums, blog posts, chatrooms, etc.), consider the risk that such statements may be unintentionally attributed to Databricks, or seen as an endorsement by Databricks. You must get approval from Your manager and the Public Relations team before accepting any public speaking engagement where You will discuss Databricks, its products, or Your role.

All employees are expected to submit certain sensitive communications and content for Legal review in accordance with our [Guidance for Legal Review of External Communications](#). More generally, employees should review and the [Brickster Communications Guidelines](#) and [Insider Trading Policy](#) before making any external communication or disclosure relating to Databricks.

If You have any questions about this policy or want to submit a statement for review, please email Public Relations at [REDACTED] or our Corporate Communications team at [REDACTED].

## Brand

The Databricks brand is a valuable asset of our company, and we are all responsible for protecting it from unauthorized and inappropriate use. You may not give permission to any supplier or other party to use the Databricks name, logo, or other branding in its advertising, promotional materials, customer references, or the like, without approval from Marketing. Browse our Brand Portal ([go/brand](#)) for general information and assets and, to seek approvals or guidance, reach out to [REDACTED].

## Social Media Policy

Social media carries the same risks as other forms of communication and expression, and Databricks employees are expected to use good judgment and follow all applicable company policies when blogging or using social media. In particular, employees must not post material that is harassing or discriminatory (see our [Discrimination, Harassment & Retaliation Prevention Policy](#)), constitutes cyber-bullying (see our [Health & Safety Policy](#)), violates our [Security, Privacy and Data Protection Policies](#) or Corporate Communications Policy (see above), or divulges Databricks or

customer confidential data, intellectual property or trade secrets. Additionally, employees should not use Databricks' name or logo in any social media identifiers (e.g., handle, username, screen name, etc.)

Consult our [Brickster Communications Guidelines](#) for more information. You may also reach out to our Corporate Communications team at [REDACTED] with questions.

## Truthful Advertising and Marketing

Databricks has a legal and ethical responsibility to ensure that all of our advertising is truthful and not deceptive. Databricks employees, particularly those involved in sales or marketing activities, must ensure that we do not make false or misleading statements about Databricks' products and services, or the products and services of Databricks' competitors, and that any public statements made are substantiated with reasonable supporting data. These obligations also apply to any social media "influencers" or anyone who may endorse Databricks' products.

# Partnerships & Contracting

## Working with Third Parties

In some circumstances, third parties can expose Databricks to serious legal, reputational, or other risks. We therefore expect the parties we work with – whether vendors or suppliers, partners, or anyone else – to behave ethically and consistent with the same high standards of conduct we expect of our employees.

Employees who hire or oversee third parties are expected to follow all rules for selection and management of these parties, as defined by the relevant Databricks teams. We also ask everyone, whether or not You manage a third party, to stay vigilant for warning signs of misconduct by third parties, whether during onboarding, in the conduct of business activities, during payment processes, or at any other time.

Consult [go/ethics](#) for more information on third-party risks, including some [Warning Signs in Third-Party Relationships](#).

## Suppliers

Databricks chooses its suppliers objectively, based on the merits of their products, services, prices, and business practices

All suppliers must be appropriately vetted to ensure that their business practices do not violate local laws, are consistent with company policies, and will not harm our reputation. Supplier agreements must be negotiated in conjunction with Databricks' Procurement and Legal teams to make certain they reflect the best possible pricing, serve Databricks' interests, and protect Databricks' reputation.

Consult our [Procurement Policy](#) or contact [REDACTED] for more information.

## Partner Program Vetting/Managing

Databricks maintains specific rules and programs for selection, vetting, and lifecycle requirements for partners. Contact [REDACTED] for more information.