

Code of Conduct

Owner	[People owner role]
Approved by	[Policy approver role]
Effective date	[Effective date]
Next review	[Next review date]
Version	1.0

1. Purpose and scope

This Code of Conduct sets the standards of behavior [Company name] (the "Company") expects from everyone who works for it. It explains what the Company requires, where to go for help, and what happens when the standards are not met.

The Code applies to all employees, officers, contractors, interns and temporary staff of [Company name] (together, "personnel"), wherever they work and whether they work on site or remotely. Contractors are bound by it through their engagement terms.

The Code owner is the [People owner role]. The Code does not list every situation. Where it is silent, personnel use good judgment and ask their manager or the Code owner before acting.

2. Our values

[Company name] expects personnel to act on these values in their daily work:

- Integrity: we are honest with customers, colleagues, auditors and each other, and we do not misstate facts or hide mistakes.
- Respect: we treat every person with dignity, regardless of role, background or opinion.
- Care for customer trust: customers give us their data to run our product; we protect it as if it were our own.
- Accountability: we own our decisions and raise problems early, including our own errors.
- Compliance: we follow the law, our contracts and Company policies.

3. Conflicts of interest

A conflict of interest exists when a personal interest could influence, or appear to influence, a decision made for the Company. Personnel avoid conflicts where possible and disclose them where they cannot be avoided.

Personnel disclose the following in writing to the [People owner role] before acting, and again whenever circumstances change:

- A financial interest in a customer, supplier, partner or competitor, other than a holding of less than 1% in a publicly traded company.
- Outside employment, consulting, advisory or board roles, paid or unpaid, that relate to the Company's business or use Company time or resources.
- A close personal or family relationship with a person they hire, manage, or select as a supplier.
- Any business opportunity discovered through their work at the Company that they wish to pursue personally.

The [People owner role] records each disclosure and, with the [Policy approver role], decides whether the activity may continue and on what conditions. The decision is recorded with the disclosure.

4. Gifts, hospitality and bribery

Personnel do not offer, give, request or accept anything of value to improperly influence a business decision. This applies to cash, gift cards, travel, entertainment, jobs for relatives and donations made on someone's behalf.

- Cash and cash equivalents are never accepted or given, at any value.
- Modest gifts and ordinary business meals are permitted when they are infrequent, openly given and not tied to a pending decision.
- Any gift or hospitality given or received with a value above the disclosure threshold below is reported to the Code owner within 5 business days.
- Nothing of value is given to a government official without prior written approval from the [Policy approver role].

Gift and hospitality disclosure threshold (per item, per person): [Gift and hospitality disclosure threshold (per item, per person)]

5. Confidentiality and data handling

Personnel have access to confidential information belonging to [Company name], its customers and its partners. This includes customer data processed in our systems, source code, security configurations, financial information, and personal data about colleagues.

- Personnel access only the information they need for their role and use it only for Company purposes.
- Information is handled according to the Data Classification Standard, including its rules for storage, sharing and disposal.
- Customer data is never copied to personal devices, personal accounts or unapproved tools, including public AI services.

- Confidential information is not discussed in public places or on open channels where others can overhear or read it.
- Suspected loss, exposure or misuse of information is reported to the [Security owner role] immediately.
- Confidentiality obligations continue after a person leaves the Company, and all Company information is returned or deleted on departure.

6. Acceptable use of company systems

Company systems include laptops, accounts, email, chat, source repositories, cloud environments, and any service the Company pays for. They are provided for business use.

- Personnel keep credentials private, use a password manager, and enable multi-factor authentication on every account that supports it.
- Personnel do not share accounts, bypass security controls, disable endpoint protection or install unapproved software on Company devices.
- Company devices are kept updated, encrypted and screen locked when unattended, as configured by the [IT owner role].
- Limited personal use is permitted when it does not interfere with work, does not break the law and does not put Company data at risk.
- Company systems are never used to harass, to access illegal or sexually explicit material, or to run a personal business.
- The Company monitors its systems for security and compliance purposes to the extent the law allows. Personnel have no expectation of privacy in Company accounts.

7. Harassment and discrimination

[Company name] provides a workplace free from harassment, discrimination and bullying, in person and online. Decisions about hiring, pay, promotion and discipline are based on merit and business need.

The Company does not tolerate discrimination or harassment based on race, color, religion, sex, pregnancy, sexual orientation, gender identity or expression, national origin, age, disability, genetic information, veteran status or any other characteristic protected by law.

- Harassment includes unwelcome conduct, comments, jokes, images or physical contact that create an intimidating, hostile or offensive environment.
- Sexual harassment includes unwelcome advances, requests for sexual favors and any conduct of a sexual nature that affects a person's work.
- These rules apply at Company events, on business travel, and in Company chat and video calls.

8. Reporting concerns

Personnel report any actual or suspected breach of this Code, of Company policy or of the law. Reports can be made to a manager, to the Code owner, or through the confidential channel below. Reports may be made anonymously where the channel allows it.

Confidential reporting channel:

Reports that involve a manager or the [People owner role] can be made directly to the [Policy approver role]. Reports that involve the [Policy approver role] can be made to the board or an outside adviser named here:

Escalation contact for reports about senior leadership:

[Company name] does not retaliate against anyone who raises a concern in good faith or who helps with an investigation, even if the concern is not substantiated. Retaliation is itself a serious breach of this Code.

9. Investigation and discipline

Reports are reviewed by the [Policy approver role] and the [People owner role]. A person named in a report, or with a conflict, does not take part in reviewing it.

1. The reviewer acknowledges the report to the reporter within 5 business days where the reporter is identifiable.
2. The reviewer assesses the report and decides whether to investigate, and who investigates.
3. The investigation is carried out promptly, fairly and as confidentially as the facts allow.
4. The outcome and any action taken are recorded and retained for at least 3 years.
5. The reporter is told that the matter has been closed, subject to the privacy of the people involved.

Breaches of this Code lead to disciplinary action proportionate to the breach, up to and including termination of employment or engagement. Breaches of law may be referred to the authorities.

10. Review of this Code

The [People owner role] reviews this Code at least once a year, and after any significant change in the business, the law or a serious breach. The [Policy approver role] approves each new version. Personnel are notified of material changes and acknowledge the new version.

11. Acknowledgment

Every person covered by this Code signs this acknowledgment within 30 days of starting and again each year. The [People owner role] keeps signed acknowledgments for the duration of employment or engagement plus 3 years.

I have received and read the [Company name] Code of Conduct. I understand it, I agree to comply with it, and I understand that a breach may lead to disciplinary action up to and including termination. I know how to report a concern and that [Company name] does not permit retaliation for good faith reports.

Employee

Name:

Signature:

Date:

Source

Source: free template from www.polaralabs.com/templates/code-of-conduct (CC BY 4.0).