Code of Business Conduct Policy

Version 1 - Approved by Rishabh

Contents

1. Objective
2. Scope
3. Policy Statement
4. Guidelines
5. Reporting Violations
6. Document security classification
7. Non Compliance
8. Responsibilities
9. Schedule
10. Version History

1. Objective

Superhawk AI's Code of Business Conduct policy outlines the company's expectations regarding employees' behavior towards their colleagues, supervisors, and the overall organization.

Superhawk AI promotes freedom of expression and open communication. All staff members are expected to follow the code of conduct. Staff members should avoid offending others, participating in serious disputes, and disrupting our workplace. Superhawk AI also expects all staff members to foster a well-organized, respectful, and collaborative environment.

This policy outlines the expectations for all Superhawk AI staff and the consequences for unacceptable behavior.

2. Scope

This policy applies to all Superhawk AI staff members, including full-time and part-time employees, contractors, and temporary workers who perform work for Superhawk AI. It applies to conduct occurring in the workplace, at company-sponsored events, and in any work-related communication channels and systems used by the company (including Google Workspace, GitHub, and company-managed cloud environments on AWS and GCP), as well as conduct on personal devices while performing work-related duties.

3. Policy Statement

Superhawk AI is committed to creating and maintaining a professional and respectful work environment. This policy describes the desired behavior of all staff members and emphasizes the importance of diversity and inclusion in the workplace.

4. Guidelines

- Be welcoming, friendly, and patient.
- Be considerate. Other people will use your work, and you, in turn, will depend on the work of others. Any decision you make will affect users and colleagues, and you should take those consequences into account when making decisions.
- Be respectful. Not all of us will always agree, but disagreement is no excuse for poor behavior and manners. Everyone experiences some frustration occasionally, but one cannot allow that frustration to become a personal attack. It's important to remember that an organization where people feel uncomfortable or threatened is not productive. Superhawk AI Staff should be respectful when dealing with other staff.
- Be careful with the words that you choose. Remember that sexist, racist, and other exclusionary jokes can offend those around you. Be kind to others. Do not insult or put down others. Behave professionally. Remember that harassment and sexist, racist, or exclusionary jokes are inappropriate for the organization. Such unacceptable behavior includes, but is not limited to:
    - Violent threats or language directed against another person. Discriminatory jokes and language

    - Posting sexually explicit or violent material.
    - Posting (or threatening to post) other people's personally identifiable information ("doxing"). Personal insults, especially those using racist or sexist terms.
    - Unwelcome sexual attention.
    - Advocating for or encouraging any of the above behavior.
    - Repeated harassment of others. In general, if someone asks you to stop, then stop.
- When there is a disagreement, efforts should be made to try to understand why. Social and technical disagreements happen all the time, and Superhawk AI is no exception. Disagreements and differing views must be resolved constructively. Remember that everyone is different. Different people have different perspectives on issues. Being unable to understand why someone holds a viewpoint doesn't mean they're wrong. Remember that it is human to err. Blaming each other doesn't help. Instead, offer to help resolve issues and to help learn from mistakes.
- The company requires that all staff members demonstrate commitment to impartially treating all people and organizations with whom they come into contact or conduct business. Unsolicited gifts or entertainment may only be accepted if they do not go beyond common courtesy and do not have a risk of influencing any business decisions.
- Superhawk AI requires all staff members (including senior management) to disclose any personal relationships, business transactions, and related parties that might cause reputational/financial harm to the organization while benefiting them.
- Superhawk AI requires all staff members that they do not offer, give, receive, or solicit anything of value to influence an official act by a public official, agent, or government employee.
- Superhawk AI prohibits all staff members from bribing foreign officials as well as making unauthorized facilitation payments to those individuals involved in customs, permitting the flow of goods and other activities.
- Superhawk AI maintains a confidential reporting mechanism for concerns about misconduct, policy violations, or legal breaches. Reports may be submitted via the company’s designated reporting email maintained in Google Workspace or through an internal reporting channel; the current reporting contact is hr@ (or an alternative channel published to staff). The mechanism supports anonymous submissions where available, and the company will investigate reports with discretion and will not tolerate retaliation against individuals who report in good faith.
- Our disciplinary policy is designed to ensure a fair and consistent approach to addressing any breach of company policies, misconduct, or failure to meet performance expectations. Disciplinary actions may include as below depending on the severity of the violation.:
    - verbal or written warnings,
    - suspension,
    - reprimand,
    - demotion,
    - termination for more serious offenses,
    - detracting of benefits for a definite or indefinite time.
- The process will involve a thorough investigation of the issue, and the employee will be given an opportunity to respond to any allegations. Our goal is to address issues constructively while maintaining the standards of behavior and performance necessary for the success of the company. The company reserves the right to take appropriate disciplinary

measures based on the circumstances, always adhering to principles of fairness and respect for all individuals involved.

5. Reporting Violations

If you are a victim of or notice unacceptable behavior, notify your reporting manager, HR, or the CEO. For confidential reporting, use hr@ or the internal reporting channel published to staff. Retaliation against a person for reporting unacceptable behavior or participating in an investigation is prohibited and may result in disciplinary action up to termination.

Note that this policy does not allow retaliation against a person for reporting unacceptable behavior or participating in an investigation of any such report. Disciplinary actions listed below also apply to any such retaliation or intimidation.

6. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

7. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Human Resources is responsible for administering the reporting process, investigations, and disciplinary actions. Managers are responsible for enforcing the policy within their teams. All staff members are responsible for complying with the policy and reporting violations. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

9. Schedule

This document is to be reviewed annually, aligned with the company's ISO 27001 and SOC 2 review cycles, and whenever significant changes occur in the organization or applicable laws (including GDPR).

End of Code of Business Conduct Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026