SHAKIL CO. PVT LTD

- **Do:** Respect Privacy: Always respect the privacy of colleagues and clients. Do not share personal or sensitive information unless absolutely necessary and authorized.
- **Do:** Maintain Data Security: Use ChatGPT only on secure networks. Ensure that all data shared with ChatGPT is encrypted and follows company data security protocols.
- **Do:** Promote a Positive Work Environment: Use ChatGPT to foster a positive and supportive work environment. Encourage constructive feedback and collaboration.
- **Do:** Uphold Non-Toxicity: Ensure all interactions via ChatGPT are professional and free from toxic language or behavior.
- **Do:** Prioritize Employee Safety: Use ChatGPT to enhance workplace safety by sharing relevant information and resources securely.
- **Do:** Follow Anti-Harassment Policies: Adhere to the company's anti-harassment policies. Report any misuse of ChatGPT for harassment or discriminatory behavior.
- **Do:** Encourage Ethical Behavior: Use ChatGPT ethically. Report any instances of unethical behavior or misuse of the tool.
- **Do:** Be Transparent: If using ChatGPT for customer or client interactions, always be transparent about the use of AI in communications.
- **Do:** Participate in Regular Training: Participate in regular training sessions on the proper and ethical use of ChatGPT.
- **Do:** Secure Authentication: Always use secure authentication methods when accessing ChatGPT.


- **Don't:** Share Confidential Information: Do not share confidential company information, trade secrets, or sensitive data with ChatGPT without proper authorization.
- **Don't:** Harass or Discriminate: Do not use ChatGPT for any form of harassment, discrimination, or bullying. This includes offensive jokes, comments, or slurs.
- **Don't:** Cause Data Leaks: Do not use ChatGPT to disseminate unauthorized or sensitive information that could lead to data breaches or leaks.
- **Don't:** Engage in Fraudulent Activities: Do not engage in or encourage any fraudulent activities using ChatGPT. This includes creating fake identities or misleading information.
- **Don't:** Use Maliciously: Do not use ChatGPT for any malicious activities, such as hacking, phishing, or spreading malware.
- **Don't:** Bypass Security Protocols: Never attempt to bypass or undermine the company's security protocols while using ChatGPT.
- **Don't:** Access Unauthorized Data: Do not use ChatGPT to gain unauthorized access to company systems, data, or networks.
- **Don't:** Make Personal Attacks: Do not use ChatGPT to make personal attacks or engage in arguments with colleagues or clients.
- **Don't:** Plagiarize Content: Do not use ChatGPT to plagiarize content or generate work that violates intellectual property laws.
- **Don't:** Use Excessively: Use ChatGPT efficiently and effectively. Avoid excessive or unnecessary use that could disrupt workflow or productivity.