
Social Media Policy For Employees

1.0 Policy Objective & Scope

The objective of this policy is to protect the company's reputation, safeguard confidential information, and ensure that all employee social media activity aligns with Canadian privacy laws (PIPEDA) and professional standards. This policy applies to all employees, contractors, and interns of the manufacturing company, whether using personal or company-provided devices, during or outside of work hours.

2.0 Roles & Responsibilities

- **HR Manager:** Responsible for communicating the policy during onboarding, handling violations, and maintaining records of policy acknowledgements.
- **IT Administrator:** Responsible for monitoring company social media accounts, enforcing technical controls (e.g., blocking unauthorized platforms on company devices), and assisting with investigations.
- **Department Heads:** Responsible for reinforcing the policy within their teams and reporting potential breaches to HR.
- **All Employees:** Responsible for reading, understanding, and adhering to the policy in all social media activities that reference the company or its stakeholders.

3.0 Core Rules & Guidelines

- Employees must not disclose confidential company information, including trade secrets, financial data, internal communications, or unreleased product details.
- All social media posts that reference the company must include a clear disclaimer that the views expressed are personal and not those of the employer.
- Employees are prohibited from using company logos, trademarks, or branding on personal social media accounts without prior written approval from the Marketing Department.
- Harassment, discrimination, or defamatory comments about colleagues, customers, or partners are strictly forbidden and may result in disciplinary action up to termination.
- Employees must not engage in unauthorized photography or video recording within the manufacturing facility or share any images of the production floor, equipment, or personnel without explicit permission.
- Compliance with PIPEDA requires that employees do not collect, use, or disclose personal information of customers or coworkers via social media without consent.
- Any social media account created for business purposes (e.g., representing the company) must be registered with the Marketing Department and managed through the official SwitchDesk portal.

4.0 Step-by-Step Procedure / Workflow

1. HR initiates the policy rollout by scheduling a mandatory training session for all employees via the SwitchDesk internal communications module.

2. Employees attend the training session, which covers the policy rules, examples of acceptable and unacceptable posts, and the legal implications under PIPEDA.
3. After training, each employee signs an electronic acknowledgement form in SwitchDesk, confirming they have read and understood the policy.
4. IT Administrator configures company devices to block access to non-approved social media platforms during work hours, unless explicitly authorized for business use.
5. Marketing Department creates a list of official company social media accounts and shares the login credentials securely via SwitchDesk's password vault with authorized personnel only.
6. If an employee wishes to post about the company on their personal account, they must submit a request via the SwitchDesk approval workflow, including the draft post and intended platform.
7. The Marketing Manager reviews the request within 48 hours and either approves, requests edits, or denies the post, documenting the decision in SwitchDesk.
8. When a potential policy violation is reported (e.g., a colleague sees a confidential post), the HR Manager opens an investigation case in SwitchDesk, attaching screenshots and relevant details.
9. HR interviews the employee involved and reviews the post against the policy. If a violation is confirmed, HR issues a written warning or initiates further disciplinary action as per the company's progressive discipline policy.
10. For serious breaches (e.g., sharing trade secrets), IT immediately revokes the employee's access to all company systems and devices, and HR coordinates with legal counsel if necessary.
11. All investigation outcomes and disciplinary actions are documented in the employee's secure HR file within SwitchDesk, with a note on the policy acknowledgement record.
12. HR conducts a quarterly review of the policy and updates it as needed, notifying all employees of any changes via SwitchDesk broadcast and requiring re-acknowledgement.

5.0 Documentation & Compliance

1. All policy acknowledgements are stored digitally in the employee's HR folder within SwitchDesk, timestamped and version-tracked for audit purposes.
2. Training session attendance records and materials are archived in the SwitchDesk training module for a minimum of three years.
3. Approved social media post requests and their corresponding approvals are logged in SwitchDesk with a unique reference number for traceability.
4. Investigation cases are stored in a restricted-access section of SwitchDesk, accessible only to HR and legal, with a retention period of five years after case closure.
5. An annual compliance audit is conducted by the HR Manager and IT Administrator to verify that all employees have current acknowledgements and that no unauthorized social media accounts exist.
6. Audit findings are reported to senior management and used to refine the policy and training materials as needed.

Regulatory Disclaimer: This document is a generic administrative template provided for educational purposes. The end-user assumes all liability for reviewing, adapting, and validating all protocols against organizational policies.