Social Media Policy for Bank's Employees

Version 3.1 (Updated in September 2021)

Index

1. Introduction

- Bank had launched its presence in Social Media with official pages on Facebook, Twitter on 1st January 2016. This social media presence has been extended to YouTube on 1st April 2016; Instagram on 18th July 2017 and it was extended to LinkedIn 01st January 2018.

- Social media use has become ubiquitous with today's consumers and has empowered them to become creators and consumers of online content. Before social media came along, consumers were primarily forced to listen to messages directly from organizations. Banks were "pushing" brand and product information to consumers via traditional media outlets. Yes, word-of-mouth has always been involved as well, but not to the extent that it is today. Social media is an extension of word-of-mouth delivery. Today, consumers pull the information they want, when they want it. Consumers trust peer opinions, product reviews and feedback from friends and family above advertisements or any other form of external information pushed to the public by the organization. The rise of social media, therefore, means that our responsibilities as a Bank have become more complex especially in the realm of customer interaction.

- Social media is often thought of in terms of a handful of well-known social media sites, such as Facebook, Twitter, and so forth, but it is actually much more than these few sites. Social media encompasses the Internet technologies that enable consumers to easily share content online, including but not limited to, social networks, blogs, videos, photos, wikis, online reviews, online check-ins and more. There are thousands of social channels, networks and media tools and the list is growing. However, the Bank has considered the following popular Social Media Channels only viz. Facebook, Twitter, YouTube, Instagram, LinkedIn and WhatsApp for this policy. This social media policy is also applicable for all other social media platforms that the bank may or may not be present on, in the future.

2. Purpose:

The purpose of having a Social Media policy in place is enlisted below:

- Do's and Don'ts of Social Media for Employees, consultants, contractors, trainees, part time and fixed time employees and casual and agency staff.
- To update and caution the employees about the consequences of violating the Bank's social media policy.
- Regulations, Legal and compliance involved in implementing social media.
- Provide guidelines for information security.

3. Management of Social Media

- Bank has engaged the services of an external agency for setting up and managing Bank's presence on Social media platforms for the Organization.
- An External Team from Agency along with a Core Internal Team from Bank is working for managing Bank's Social Media Presence.
- Bank's Social Media presence has been launched on Facebook, Twitter, YouTube, Instagram and Linkedin.

- The Social Media Team of the Bank may be reached by email at social. media@bankofbaroda.com

4. Policy for Employees:

Employees are our brand ambassadors in some way. What one says in their individual capacity, about the Bank and in general, on public platforms on social media reflects on our brand image. Employees should keep this in mind no matter which forum they are posting on. There have been cases where Brands have been publicly censured due to hateful comments by employees in their individual capacity. Employees are not allowed to put such types of comments which may adversely affect the Bank's image.

- The Bank has a separate Team for managing Bank's social media platforms. Except for the team, no employee is allowed to post any content on purporting to be on behalf of the Bank on the internet.
- For centralized monitoring purpose, no employees should, without taking written approval from the social media team, express any view on any internet site or social media about the working of Bank of Baroda or the business of Bank of Baroda or generally about Bank of Baroda or any of its officials.
- **No employee should without taking approval from the competent authority (as defined in the communication policy of the Bank) express views or opinions on behalf of the Bank or in the official capacity of his position in the Bank.**
- No employee of the Bank should create or promote any group, community or webpage which will use the name or logo/identifier of Bank of Baroda or become a member of any unofficial such group/ community or web page.
- If the employee comes across any such unofficial/ spurious group or community, the same should be reported to the social media team so that the appropriate legal action including reporting of such unofficial / spurious group to safeguard bank's interest may be done by the Social Media Team.
- No employee should post anything on any social media platform or websites, things that would damage the reputation of the Bank or any of its employees.
- No employee in their official capacity should write or express anything that would be defamatory to the Bank or its employees on any social media platform or websites.
- No employees should express negative views or criticize Bank Management, policies or strategies on social media platforms or websites.
- No employees should engage in collusive behavior on any social media Platform, with Bank's competitors or employees.
- Any staff members of the bank found creating alternate ids/fake ids and escalating grievance issues in the public domain by tagging the bank's higher authorities will be treated as the violation of the Social Media policy for employees and may be meted out strict action as deemed fit by the competent authority.
- No employee should post or forward or discuss views which are indecent, derogatory, abusive, immoral, unparliamentary and vulgar, without knowing full fact and background of any matter or against the organization/ Bank/ any individual or against the Government or any Constitutional Body. The post/ forward/ comment, must also not be provoking/ instigating people to commit any act(s) which do not fall under proper behavior/ conduct norms/ guidelines or are illegal or criminal in nature.

Using social media at work:

- Bank of Baroda understands the importance of the internet in shaping the general public opinion about its services, employees and customers. Our Bank also realizes the importance of staff joining in helping shape the industry conversation and direction through interaction in social media.
- Using social media for personal use during office hours should not interfere with business and office commitments and should be minimal.
- Employees should remain aware of how their personal use of social media during working hours reflects upon them and the Bank.
- Employees should not use our Bank's e-mail addresses to register on social networks, blogs, or other online tools utilized for personal use.
- When using online accounts you must ensure that your @bankofbaroda.com email address is not exposed to the public/ Social Media platform. Do not create any online account or profile that implies such account or profile is connected to or owned by Bank without Bank's prior consent.

General Advisory for Using WhatsApp:

The Do's

- Employees can make internal groups/teams to discuss ideas, co-ordinate task, seek help & inputs on specific business agenda that they are working on to drive the business etc.
- Sharing articles of interest and value which are beneficial to the staff members of this group.

The Don'ts

- Do not share post/views which are indecent, derogatory abusive, un-parliamentary and even vulgar in language in any communication.
- Do not share internal circulars & policies with any third party (other than Bank's employees) as it harms the Bank's competitive position with respect to its competitor banks.
- Do not share confidential matters, orders & strategies of our Top Management with any third party (other than Bank's employees).
- Do not use un-parliamentary language, insulting others or obscenity
- Do not write express anything on WhatsApp which may be defamatory to the Bank or officials or its employees in their official capacity or which is in the form of accusations.
- Do not publish rumors and/ or internal and/ or confidential information about the Bank or related third parties on social networks (customers, employees, collaborators) that can have a negative impact on the Bank's image and reputation.
- Do not use Bank's logo/identifier or nomenclature in the display picture or group name etc.
- No employee should forward or discuss messages/ views without official confirmation or knowing authenticity or full fact and background of any matter against the organization/ Bank/ any individual or against the Government or any Constitutional Body.

Rules of use of social media:

- Keep personal and professional life separate.
- Do not post, forward or upload or share a link to any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.
- Any member of the staff who feels that they have been harassed or bullied or are offended by the material posted or uploaded by a colleague onto a social media site must inform the social media team and HR team immediately for investigation and taking further action, if appropriate.
- Never disclose commercially sensitive, anti - competitive, private or commercial information. If unsure whether the information shared lies within any of the above mentioned categories, please consult the social media team.
- Do not post, forward or upload anything belonging to a third party without that third party's consent.
- When in doubt about a link, please do not share. You can consult the social media Team to clear your doubts at social.media@bankofbaroda.com. Before including a link to a third party website, check whether any terms and conditions are involved in linking the website. All links must be done so that it is clear to the user that they have moved to the third party's website.
- Employees should pay special attention to intellectual property and personal data protection before posting. Read before complying with its terms of use/ acceptance guidelines of social media sites.
- On the Bank's website or social media sites, do not share posts or upload links to chain mail, junk mail, cartoons, jokes or gossip.
- Employees should be mindful of the impact of anything they post over social media, as it also reflects on people's perception of the Bank.
- Employees responsible for the content published in the social media tool should be alert that whatever is published will be public for many years and it would be impossible to take it down entirely from the internet e.g. individuals can take screenshots of the content and circulate it.
- Never mention the details or any information pertaining to colleagues, customers or suppliers without their prior written permission.
- Always consider others privacy and avoid discussing topics that might be inflammatory, controversial, e.g. politics and religion.
- Avoid discussing contact details where they can be accessed and used publicly.
- Posting rumors, internal and confidential information can lead to legal action against the employee.
- Under no circumstances whatsoever, is the use of pseudonyms or false names advisable.
- Inter-personal issues between colleagues or between a superior authority that give rise to resentment or grievances must be taken up through Bank's established grievance channels only and not posted in Social Media for circulation at large.
- Decency and basic etiquettes must be maintained in all modes of communication.

The Do's:

- Make your social profile in your personal capacity and use it with responsibility.
- If you comment on matters related to your work, use a disclaimer stating the views are your own and not of your employer / Bank.
- Avoid transgression of any other person's rights.

- Be aware of the Bank's service conditions, statutory and regulatory guidelines, business ethics etc. before randomly commenting on any issue.
- Do model behavior- Our online activity may feel private, but we all know it leaves a permanent mark in a public space.
- Do promote good work – Yammer offers many ways to grow the reach of our good work, talent and positive outlook. We may take advantage of these benefits as long as we do it the right way and allow the traffic to grow organically.
- Employees and associates are encouraged to RT (Retweet), Share (on Facebook, LinkedIn etc.), any brand posts made by the Bank. This improves our brand visibility and helps the image.
- If an employee has any grievances, it should be raised via the established internal channels.

The Don'ts:

- Do not create fictitious profiles and do not post anonymous comments
- Do not use un-parliamentary language, insulting others or obscenity in any communication.
- Do not make any false, misleading or defamatory statements concerning your work or the organization.
- Do not canvass for any donation, lottery or third party marketing / business promotional activities / affairs on any interest site or social media.
- Do not write / express anything on Social Media which may be defamatory to the Bank or officials or its employees in their official capacity or which is in the form of accusations.
- Do not publish rumors and / or internal and / or confidential information about the Bank or related third parties on social networks (customers, employees, collaborators) that can have a negative impact on the Bank's image and reputation.
- Do not criticize just for the purpose of criticizing and just because some other practice is continuing in some other organization. We must try to understand the rationale behind the Bank's actions / policies initiated and give feedback, if any, for further improvement.
- Avoid responding to Customer grievances on social media forums. There are established processes put in place by the Marketing (Social Media Team) in collaboration with the Customer Service Team. These processes should be followed. If any employee has any knowledge of a specific customer grievance, please share with the Customer Service team via email/internal communication but certainly not on public (social media/ WhatsApp) forums.
- If an employee has any grievances, it should not be raised via social media channels.

Monitoring of social media:

- Employees should watch for phishing attempts, where scammers may attempt deception to obtain information relating to either the Bank or its customers.
- Employees should avoid clicking on links in posts, updates and links which look suspicious.
- Employees should be aware that any use of social media websites may be monitored and where breaches of the policy are found, action may be taken by the Bank.

- Posting, uploading or forwarding any kind of material mentioned in the list below, whether in personal or professional capacity will amount to gross misconduct.
    a. Pornographic material (writing, pictures, videos, memes)
    b. A false or defamatory statement about any person or Bank.
    c. Material which is offensive, obscene, criminal, discriminatory, or derogatory may cause embarrassment to the Bank.
    d. Confidential information about customers, staff members or the Bank.
    e. Any other statement which is likely to create any liability (criminal/civil for the staff member/Bank)
    f. Material in breach of copyright or other intellectual property rights or which invades the privacy of any person

- This policy covers all individuals working at all grades (whether in India or outside India) including management, directors, employees, consultants, contractors, trainees, part time and agency staff.
- All staff are expected to comply with this policy at all times to protect the privacy, confidentiality and interests of the Bank and its services, employees, partners, customers and competitors.
- While an employee connects with any customer / supplier/ vendor/ consultants/ contractors/ trainees on Facebook, Instagram, LinkedIn, Twitter, YouTube, WhatsApp etc., he/ she should comply with the Social Media Policy of the Bank, which should be read, understood and complied in full congruence with:
    - Bank of Baroda Officer Employees' (Conduct) Regulations, 1976
    - Bank of Baroda (Officers') Service Regulations, 1979
    - Should Not violate the obligation of fidelity and secrecy casted on bank under section 13 of 'The Banking Companies (Acquisition and Transfer of Undertakings) Act, 1970
    - Bank's Circulars on Social Media Policy for Employees BCC:BR:108:3 dated 01.01.2016, BCC:BR:108:584 dated 01.12.2016, BCC:BR:109:541 dated 18.10.2017, HO:BR:110:209 dated 24.10.2018 and all other guidelines issued time and again by the Bank regarding conduct of employees on Social Media.

5. Violation Consequences

- Wherever breach of Policy is noticed and / or reported, it will be forwarded to the concerned Disciplinary Authority for the employee who breached, for appropriate action. If the Disciplinary Authority has decided to initiate disciplinary action, it will be a "non- vigilance" case, unless financial / vital information is disclosed which may lead to financial loss to the Bank or customer.
- Where evidence of misuse and violation of this policy is found, the Bank may initiate suitable action under the Law / Service Regulations against the concerned employee as deem appropriate.
- Deliberately breaching this policy is a serious matter and employees who do so will be subjected to strict disciplinary action under the relevant Service Regulations Viz. Bipartite Settlement dated 01.04.2002 and Bank of Baroda Employees' (Discipline & Appeal) Regulations, 1976 etc. and may even lead to termination of the employment

- Ignorance of the policy or its guidelines also cannot be allowed as an excuse to breach the Social Media policy.
- If any staff notices any violation of the Social media policy, he/ she should bring this to the notice of the Bank/ Social Media Team at social.media@bankofbaroda.com
- Violations of Social media policy can also tantamount to action/ prosecution (civil/ criminal) by external authorities under the Act or provisions of any other Act in force.
- Employees, contract workers and other users may also be held personally liable for violating this policy.
- Where appropriate, the Bank will involve the police or other law enforcement agencies in relation to breaches of this policy.

6. Regulations, Legal and compliance:

Applicability of Law:

Laws that are governing Information and communication technology affairs will also be applicable for setting up social media in the organization.

- Defamation Law, The India Penal Code, 1860 under section 499 and 500, describes the basis for harming the reputation of a person. Bank and its members of staff should ensure that their personal emotions/frustrations/ anger is not expressed on social media platforms as it could go viral. The language should be professional and if posted officially, the language needs to be validated by the social media Team before posting on any website.
- Leveraging the guidelines mentioned in 'Know your customer' (KYC) norms/ Anti-money Laundering (AML) standards/ Combating of Financing of Terrorism (CFT)/ Obligation of Banks under PMLA,2002 dated 2nd June,2012, any person from the Bank can use Social Media as an additional form for validating customer identity but cannot use the profile data for cross selling.
- Reserve Bank of India continues to be the regulator for any payment/ Fund transfer process initiated through Social Media channels as per Payment and Settlement System Act, 2007. Our Bank will have to comply with settlement and reporting requirements as detailed in the Act.
- The social media Apps of our Bank for financial/ non-financial transactions will comply with National Cyber Security policy, 2013 and ensure a secure computing environment.
- India does not have a Privacy law yet. However as per section 43A and section 72A of Information Technology (Amendment) Act, 2008, our Bank will adopt reasonable security practices to ensure sensitive personal data or information is not compromised. Rules notified under section 43A defines the privacy and security requirements.
- "The Right to Information Act, 2005 Section 8(1) (j)" exempts disclosure of personal information which has no relation to any public activity or interest or which could lead to unwarranted invasion of privacy of the individual. Hence, sharing customer details on loans, deposits, etc., over social media sites for more referrals should be avoided.
- In the case of social media analytics tools being used, that would provide customer interaction / behavior data. Such information cannot be disclosed. As per, " The Right to Information Act, 2005, Section 8(1)(e)" information available to a person in his fiduciary relationship cannot be shared unless it is for Larger public interest as decided by a competent authority (Reserve Bank of India).
- "The telecom Commercial Communication Customer Preference Regulations, 2010" of the TRAI, details the method for curbing the growing menace of SMS and

unsolicited calls. Our Bank having customer contacts through social media sites should not violate the TRAI regulations.

- Incase if employees make extremely derogatory and inflammatory comments, the same shall be punishable as per the Section 66A to 66F of Information Technology (Amendment) Act, 2008. (By creating social media properties the organization is likely to fall under the category of 'intermediary' as it would provide end users to update/share comments on its property. The obligations for the intermediary have been defined separately under Section 79.)

Ethics of Data Usage

- Collection, accessing, processing, storing and sharing of data has to be done very cautiously in order to prevent any misuse.
- While collecting and using information, it should not harm the end user/ customer. Ethical practices should be followed in case of using this data for business purposes.
- Collection of Information should be fair and informed choices should be provided for usage of this information.

7. General Advisory: Information Security guidelines:

Access Management

- Employees should use their personal Email ID (Non- official) for each Social Media Site and to adopt best practices for password security.
- Do not share Email ID or password used at a social media site. Use separate Email ID and password for each social media platform.
- Implement mailbox spam and content filtering.
- Access should be restricted to the role assigned to each individual in the social media field like the content/campaign designer/ approver, publisher.
- Remote Desktop connections to the system/ computer used for social media interactions should not be allowed.
- The external agency helping in setting up a social media platform for the Bank should have restricted access to confidential data. Bank should review third party security controls annually.
- Employees should record the current and previous login details and validate the postings for every logon.
- Employees should perform re- authentication to connect to social media apps or on session timeouts. Implement CAPTCHA/ Virtual KeyBoard - based authentication.
- Employees should keep computers/ mobile/ smart phones up - to - date and virus free.
- Employees should clear all browser history and cookies and other temporary files before and after accessing social media sites.
- Employees should implement IDS, IPS, Firewalls, web content filters, layered proxies for data being posted on social media platforms from the Bank.

Monitoring and Logging

- Employees may continuously monitor for Fraud/Cloned sites using social media analytics tools and should reach out to social media team (at

social.media@bankofbaroda.com) of Marketing Department - to bring down cloned/ fraud sites.

- Employees may use Google alerts, social mention and other Social Media analytical tools to get an update on what is being discussed/ commented about the Bank.
- Employees may track comments and conversation about the adopted social media platform as the platforms might be going through information security issues.
- If there is spamming on Bank's social media site page, the employee should immediately contact the social media site/ team and should not send email/ message to the person posting it.

8. Monitoring and review of policy:

- The Marketing Department will be responsible for reviewing this policy at any point of time as felt necessary, to ensure that it meets legal requirements and reflects best practices.
- In case of sudden changes in the social media or Banking industry, a meeting can be held to bring in the desired changes in the policy, on urgent basis.
- MD/CEO (or) Executive Director would be the competent authority to approve changes in the policy.
- The Policy shall be in force till 30.09.2024.