



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



**Project Report
on
Social Media Policy
for
Police Organisations
(Project No.01/MM:06)**

Prepared by
Micro Mission 06 (Proactive Policing & Visualizing Future Challenges)
National Police Mission
2020-21

Bureau of Police Research and Development
Ministry of Home Affairs
Govt. of India

‘Promoting Good Practices and Standards’



DOCUMENT INFORMATION

Project	Social Media Policy for Police Organisations
Project No	01/MM:06
Project Leader	Dr. Shamsheer Singh, IPS
Project Team	❖ Shri Abhishek Trivedi, IPS ❖ Shri Hari K Kusumakar, IPS ❖ Shri Abhishek Dullar, IPS ❖ NPM, BPR&D
Version No.	1
Approved on	29.12.2020

Table of Contents

	<u>Page No.</u>
1.0 Introduction/Background	01
2.0 Overview	01
2.1. Project Title - Social Media Policy for Police organisations	01
2.2. Vision	01
2.3. Objectives	02
3.0 The Project	02
3.1. Purpose of the Project	02
3.2. Sponsor	02
3.3. Benefits	02
4.0 Situational Assessment and Problem Statement	03
5.0 Critical Assumptions and Constraints	04
6.0 Implementation Strategy	04
6.1 Choosing Platforms	04
6.2 Management of Social Media Vehicles	04
6.3 Account Management	04
6.4 Response and Feedback Management	05
6.5 Posting guidelines for audience	06
6.6 Resource Management	08
6.7 Content Management	08
6.8 Operational Do's and Don'ts	09
6.9 Record Management	10
6.10 Deliverables	10
6.11 Stakeholders	10
6.12 Related projects	10
6.13 Work Plan	10
7.0 Legal Provisions	11
8.0 Data & Information Security Governance	11
9.0 Provisions related to Personal Information & Security	11
10.0 Personal Use of Social Media	12

“Social Media Policy for Police Organizations”

1.0 Introduction/Background

Internet access has grown tremendously over the last few years resulting in increasing popularity of Social Media. Social Media tools have become synonymous with popular culture and new waves of Personal Communication. Law enforcement agencies world over have, therefore, realized the importance of the use of Social Media to enhance communication, streamline processes, and increase productivity.

Social Media is defined as a category of Internet-based resources and tools that integrate user-generated content and user participation. Social media is an integrated technology that allows users to generate their content and share that content through various connections. Social media is commonly associated with Web 2.0, technology that focuses on integration, collaboration, and interaction. There are numerous social media tools available, with different characteristics, user demographics and functionalities. Examples of social media tools include blogs, social networking sites, microblogging sites, photo and video-sharing sites, wikis, RSS feeds, and podcasting.

Social Media provides a new and valuable means of assisting the Police Department in achieving various policing objectives like *alerts, crime prevention, crime investigation, crime reporting, community engagement, soliciting tips*, and other related objectives. The Policy identifies use by the Police Department as an organization that can be explored and expanded by Administrative and Supervisory Officers. The Department also recognizes the role of Social Media tools in the personal lives of department personnel. Therefore, the Policy provides information about a precautionary and prohibitive nature on the use of Social Media by department personnel. Furthermore, the policy recognizes the important role of the audience on Social Media vehicles of the Police Department. Guidelines on the use of Social Media by the audience, therefore, are part of this Policy Document. Similar to the personal use of Social Media by department personnel, these guidelines are also precautionary and prohibitive. These are for the awareness of the audience so that they do not violate any of the laws.

2.0 Overview

2.1 Project Title

“Social Media Policy for Police organizations”.

The ‘Social Media Policy for Police organizations’ is a generic policy that can be suitably modified to accommodate the specific needs of concerned Police organizations.

2.2 Vision

Effective use of social media for enhanced outreach, improving the efficiency and management of positive perceptions of the police organizations by connecting with the citizens through social media channels.

2.3 Objectives

1. Objective of the policy will be to help the police organizations in using the social media channels or platforms effectively to connect with the citizens.
2. To frame the broad guidelines for Content Management, Response Management and Feedback Management.
3. Legal guidelines for use of social media by Police Organizations and individual Police Officers.

3.0 The Project

3.1 Purpose of the Project

The purpose of the project is to frame a broad policy framework and operational guidelines for effective utilization of social media in police organization.

Social Media offers a unique opportunity to Police Organizations to potentially give an interaction-based platform between police and citizens. Social Media in recent times has become synonymous with Social Networking sites such as Facebook or Microblogging sites such as Twitter and Professional Social Network like LinkedIn. Through the implementation of such a policy, will help police organizations in building trust & getting cooperation from citizens in the control of crime. Police organisations can also effectively use social media for various purposes like investigation, deriving intelligence and public outreach. This project attempt to address what needs to be achieved and addressed in a social media policy for police organizations.

3.2 Sponsor

State / Central Police organizations will implement the social media policy in their respective jurisdiction. A separate budget can be allocated for the same.

3.3 Benefits

Effective police-public outreach is crucial for Policing outcomes. Success in Policing depends to a large extent on state of Police-Public Interface. Management of public delivery communication platform is expected to improve the effectiveness of policing efforts.

Social media can be used for a variety of purposes to further the mission of police organizations.

1. **Investigation.** Social media can be used as an investigative tool when seeking evidence or information about missing or wanted persons, Open Source Intelligence and web-based crimes. Once identified, this information can then be used by law enforcement agencies to further an investigation.

2. **Community Outreach and Information.** Social media tools can be used to enhance community policing. Through community policing and with this framework agencies can promote better communications with the citizen, awareness, provide greater access to information, foster greater transparency, encourage broader participation, and provide a vehicle for collaborative problem solving. Agencies are using various social media tools to reach out to their communities in new ways and foster valuable connections throughout their jurisdictions. For example, crime prevention tips, advisory and crime reporting may be shared over social media.
3. **Advisories.** Social media also provides a number of excellent platforms for releasing time-sensitive notifications. These notifications may be related to items such as road closures, special events, natural disasters emergencies, and missing persons, etc.
4. **Fighting Fake News & Rumours.** Fake News, Rumours and Disinformation related issues can be effectively addressed through the social media. Police Organizations can utilize social media to inform the media and the community by serving as the source of correct information regarding critical incidents and distributing accurate information in a timely manner.
5. **Recruitment.** Police organizations can utilize social media tools such as blogs, social networks, and multimedia-sharing sites to provide potential applicants and recruits a unique view of law enforcement work.
6. **Managing the Perception.** Social media can help in improving the perception of the effectiveness of police organizations by sharing the positive work under a long-term strategy.

4.0 Situational Assessment and Problem statement

- a. Youths are using social media for communication, news updates and business & social interactions. Most of the youth use smartphones to access social media. Hence, police organization has no options but to use social media to connect with new smartphone generation for awareness and community policing purposes.
- b. Social media has reduced the role of the traditional media channels like news papers & TV channels in dissemination of information to the citizens. Police can use these social media channels to bridge the trust deficit between public & police by providing the correct information directly to citizens.
- c. Since social media allow two-way interaction with citizens, it can help in getting the feedback on working of police. Feedback and interactions can be very useful in calibration of police response.
- d. Social media can help in image building and branding of police organization. Sharing of positive stories & transparent communication with citizens will improve police-public relations and ultimately image will improve.

5.0 Critical Assumptions and Constraints

Social media users in India are increasing day by day. Studies of **Statista** (<https://www.statista.com/statistics/240960/share-of-indian-population-using-social-networks/>) shows that, in 2020, over 50 percent of India's population was accessing social networks. It was estimated that by 2025, this penetration of social networks would be 67 percent of the country's population. Out of which nearly all Facebook users in India accessed the platform via mobile phones as of January 2020. Only 4.6 percent of Facebook users in the country accessed the platform both from a phone and from a computer.

As social media platforms are the most used by the citizens for communication, socialization and other purposes, therefore, these platforms can become enabler for police organizations to interact with people meaningfully.

Constraints

1. Sizable population in rural areas are not using social media and cannot be reached via these platforms. Secondly, all staff of the police organizations are not well versed with handling of social media.
2. Policy on social media needs to be reviewed regularly in the context of continuous change in the use of social media vehicles.

6.0 Implementation Strategy

6.1 Choosing Platforms

Having defined the objectives, the next step is to identify platforms and phases in which such an engagement shall be undertaken at these platforms. While social networks currently seem to be the face of social media, they are not the only platform. Some of the popular vehicles in India are Facebook, Twitter, YouTube, Google Plus, etc.

6.2 Management of Social Media Vehicles

Management Structure includes Account Management, Response and Feedback Management, Resource Management, Content Management, Legal Provisions, Data and Information Security Governance.

6.3 Account Management

a. Account Creation:-

A social media account establishes an organisation's online identity. Wherever possible, the same name for different social networking accounts may be adopted to ensure ease of search on the internet. All social media sites or pages of the draft shall be approved by the Department Head or his or her designee. Social media pages shall clearly indicate they are maintained by the department and shall have department contact information prominently displayed. Social media pages should state that the

opinions expressed by visitors to the page(s) do not reflect the opinions of the department.

b. Login and password:-

Each new account requires a URL, user name and/or email address and a password. A proper record of login ids and password must be maintained. This is critical as multiple people may be authorised to post on behalf of the department.

c. Account Status:-

It is important to define whether the engagement is undertaken through official accounts only or the officials are permitted to use personal accounts also for posting official responses. It determines who says what on behalf of your organisation and in what form it is published. It also outlines how each piece of published information is presented where it is published. The most important aspect is whether the responses are in Official or Personal Capacity and there should be clarity in this aspect.

6.4 Response and Feedback Management

- a. This indicates how often would the pages/information be updated, in what manner would the responses be posted, what would be the turnaround time of responses, etc. The major attraction of social media is the spontaneity and immediacy of response and feedback and those visiting the site would expect some kind of response within a pre-defined time limit.
- b. As far as possible, all the inputs are to be promptly replied to in a professional manner. Sometimes the information desired by people may not relate to a particular department or unit. In such cases, they may be guided suitably with contact details of the appropriate person. In all cases, the response is to be given as far as possible within 24 hours. The Police Department should strive to give maximum information, which concerns the people proactively.
- c. Police Department should not assume that people are fully aware of their organisation and its functioning. Making audience aware about the organisation should be one of the key objectives while creating content.
- d. Whenever a response is required, it should be short and to the point. While employees are free to post response in their personal capacity, it is mandatory that while they are doing so, they must clearly identify themselves, confidential information must not be divulged and should not be seen to represent “official view” unless authorised to do so.
- e. While most of the responses to comments and queries may be routine, some may be required to be escalated to the Department Head for consultation and arriving at a correct response.
- f. Finally, there should be congruence between responses posted on social media and those on traditional media.

6.5 Posting Guidelines for Audience

Audience should be informed and made aware about the rules & guidelines for sending feedback and comments to avoid misunderstanding. For the purpose of simplification, the following guidelines are given for use of Social Network named Facebook by City/ District Police.

- a. The theme of the page is “Community Policing in <name>”. If we all use common courtesy and common sense then everyone will feel comfortable participating in various dialogues and interactions on this page. The purpose of this page is to encourage open, courteous communication, not accusations or judgments. Members should know that it is not just a page of <name> Police but the entire community of <name> to improve policing in <name> District.
- b. Please ask questions and let us know your concerns. We want to hear from you.
- c. Please do not use cursing or obscene language.
- d. Please do not make threatening or abusive statements, including those supporting violence.
- e. Please do not post comments that may be construed as inflammatory or derogatory towards victims, suspects or any other individuals.
- f. For emergencies call **100, 112 or 108 or Police Station Land-line numbers**. This page is not checked 24 - 7. It is checked at least once a day.
- g. When posting a request, please keep in mind that we can only respond to those posts that include the date, time and specific location of the incident. We cannot respond to posts without specific information.
- h. Members should not open anonymous and pseudonymous account to post anything in a similar manner. Do follow Facebook rules and post using a real profile and person. False person as will be banned from the page. It is for the information of everybody that all types of accounts can be traced back to the computer, mobile, etc., where they are created.
- i. It is important that the posts on this page are brief and to the point. Please avoid posting long stories. Also, please avoid voicing political opinions.
- j. If you want **to bring** out some short comings in the police department of <name> District, please do it in a specific manner quoting the incident, if any, and not in a generalised manner.
- k. If one feels that any policeman has violated some law, one should try to quote the specific incident rather than blaming the entire police of <name> District, so that he or she can be corrected and at the same time the morale of the entire police force is not hurt.

- l. If you want to express disagreement with someone's opinions, please do so objectively and politely and avoid personal criticism. Members indulging in personal attacks may be put on moderation without notice and may be unsubscribed from the page.
- m. Do not post advertisements.
- n. Do not post personal / racial / ethnic / gender-based insults or offensive comments.
- o. Do not get personal. A good general rule to follow is, "criticize ideas, not people".
- p. Do watch what you say - you are responsible for what you write. The opinions expressed by visitors to this page do not reflect the opinion of the department.
- q. If you wish to transmit information directly to <Chief> you may send it by SMS at <number> or email to <email>.
- r. The material you post on the site should not be illegal, obscene, defamatory, threatening, or abuse intellectual property rights and should not violate any law of the land.
- s. We reserve the right to moderate/delete your account and to delete any content posted by you. Members not following posting guidelines are liable to be put on moderation without advance notice and may be unsubscribed from the page. We are open to your comments, suggestions and criticism.
- t. <Name> Police Department does not remove posts without due thought and consideration. The contents of each Facebook page are at the discretion of the administrator/registered owner of the page, per Facebook guidelines. <Name> Police Department strives to be tolerant; however, in appropriate comments will be deleted.
- u. This forum is designed to share information and answer questions from the community in an environment of harmony. Constructive criticism of the <name> Police Department is welcome.
- v. <name> Police Department works within the legal system, which deems any suspect innocent until proven guilty in a Court of Law. We are proud to serve the Residents of <name> District with community policing philosophy. We appreciate the same respect and consideration from those joining us here on Facebook. Thank you for your support. Let us know how we can help. We appreciate that you want to be informed and we try to answer and acknowledge every single post. Thanks for your understanding and cooperation.

6.6 Resource Management:

Since using social media is a resource intensive exercise, it is important to ensure that resources and their responsibilities are clearly marked out very early. Both internal resources and outsourced resources can be used for managing the engagement. However, it is advisable to create a dedicated team. One of the key resources is an internal champion within the system who can lead the strategy within the department. It is important to note that since the engagement via social media requires different skill sets, the champion and other resources identified would require orientation & training specifically for the tasks assigned to them.

The roles and responsibilities of the team responsible for creating, managing and responding on social media platforms must not be limited just to responses, but also include responsibility for matters related maintenance of login ids and passwords issues related to data security, archives, privacy, etc. The officials designated for engagement with citizen using the social media should be covered under a well-defined immunity provision in consonance with the RTI Act and the IT Act and the IT Act (Amendment), 2018.

6.7 Content Management:

Content Creation & Social media profiles overlap, therefore, sharing consistent content on all social media platforms should form the bedrock of the content policy. In order to enable wider participation, content creation and availability should be in Indian languages and must not be limited to text alone.

Employees of the team authorized for posting content and engaging shall observe and abide by all copyright, trademark, and service mark restrictions in posting materials to electronic media.

A moderation policy should also be published if the platform permits others to add their own content; this informs people what they can post whilst protecting others who may visit your platform. The moderation policy should include matters related to copyright, rights to addition and deletion etc.

Department Personnel representing the department via social media outlets shall do the following:

- a. Conduct themselves at all times as representatives of the department and, accordingly, shall adhere to all departmental standards of conduct and observe conventionally accepted protocols and proper decorum.
- b. Identify themselves as a member of the department.

- c. Not make statements about the guilt or innocence of any suspect or arrestee, or comments concerning pending prosecutions, nor post, transmit, or otherwise disseminate confidential information, including photographs or videos, related to departmental training, activities, or work-related assignments without express written permission.
- d. Conduct NO political activities or private business.
- e. Social media can only be used by the Authority to communicate existing Government information and propagate official policy to the public.
- f. Great care must be taken to avoid propagation of unverified facts and frivolous misleading rumours, which tend to circulate often through miscreants on social media platforms.

It must be reiterated here that social media should only be one of the components of the overall citizen engagement strategy and government departments must desist from using only social media to communicate with their stakeholders. Initially, the departments may just aim to post information regularly. For example, if it is a Face Book Page, postings may be done at least a couple of times a week and on Twitter slightly more frequently. Ideally, none of the sites should be left more than a week or two without new content.

6.8 Operational Do's and Don'ts

Follow these instructions during operation of Social Media accounts:

- a. Know your target audience. Identify your current audience as well as potential audiences that you may not be reaching or audiences you hope to reach in the future. Social media will allow you to reach a broad audience and include new demographics in your outreach.
- b. Ask your audience to spread a word about your initiative, only if it is necessary.
- c. Do not post messages that may be prejudicial to court proceedings, abusive, defamatory, harmful, obscene, racially offensive, sexually offensive, and unlawful.
- d. Keep in mind that social media outlets do not limit you to text, consider using other types of content such as pictures and video.
- e. Online activity during working hours or using agency equipment must be primarily business related.
- f. Respect your audience.
- g. Show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory—such as politics, religion and personal life.
- h. Do not post same or similar messages more than once. This will be viewed as spam.
- i. Try to get your account verified.
- j. Use your logo/official identities as pictures to make them look credible.
- k. Connect your social media pages and accounts with your official website.

- l. If incorrect information is posted on your page, inform people about it.
- m. Allow people to post on your page.
- n. Value criticism and appreciation equally on Social Media.
- o. Respect copyright, fair use and public records laws.
- p. Stick to the time frame and make it clear by when somebody should expect a reply to a request.
- q. Keep you content fresh and up to date.
- r. Train more and more policemen in use of Social Media.
- s. Be the first to correct your own mistakes. Do not alter previous posts without indicating that you have done so.
- t. When responding to a negative post, state facts and provide supporting documentation. Avoid ongoing conversations that do not progress toward greater understanding.
- u. Set goals. As with any new initiative, it is important to set goals. Without goals, it will be impossible to determine success in the future. Your goals may be diverse, ranging from strictly numerical outputs such as page views or number of followers, to offline behaviours and actions, to overarching community themes such as reduced crime or improved police-community relations. Some of these goals may seem difficult to measure, but identify them any way.
- v. Use analytics and insights to know about the audience and their response.

6.9 Record Management:

Social media content shall adhere to applicable laws, regulations, and policies, including all information technology and record management policies. The requirements under existing legislations, e.g., RTI, etc., need to be kept in mind and are paramount in influencing decisions regarding record keeping. Records may be created on agency's internal platform and maintained with appropriate tags, e.g., creator/ sender, dates, posting site etc. Screenshots may be captured and stored in soft or hard (copy) format and filed at appropriate place. A summary may be created of the information/ consultation and filed. With advancement in memory technology, the department may ordinarily keep all the engagements other than cases where moderation is required.

6.10 Deliverables:

Deliverables will be dependent on the goals & objectives for different organizations.

6.11 Stakeholders:

Stakeholder in this project will be the concerned police organizations.

6.12 Related Projects:

No related projects.

6.13 Work Plan:

The work plan under this project shall be prepared by the implementing police organization depending on the size and type of the target audience.

7.0 Legal Provisions

The legal implications must be viewed in accordance with the law of the land, e.g., RTI Act, IT ACT 2000 & IT Act (Amendment) 2018, etc, as also rules and regulations made there under.

When a Government department provides such social media facilities on its network, receives, stores or transmits any particular electronic record on behalf of another person or provides any service with respect to that record, they become intermediary under Section 2(1)(w) of the amended Information Technology Act, 2000.

Section 79 of the amended Information Technology Act, 2000 provides the broad principle that intermediaries like Government departments providing social media facilities are generally not liable for third party data information or communication link made available by them. However, this exemption from liability can only be applicable if the said Government department complies with various conditions of law as prescribed under Section 79 of the amended Information Technology Act, 2000.

It should comply with the Information Technology (Reasonable Security Practices and Procedures & Sensitive Personal Data or Information) Rules, 2011.

The Government further stipulate that **ISO 27001** is one acceptable standard of reasonable security practices and procedures. Thus, all Government departments which are providing social media facilities must comply with **ISO 27001**. In case, the Government departments do not comply with **ISO 27001** and provide social media facilities on which network sensitive personal data is going to be stored, processed, handled or dealt with, the said Government department could be in breach of law and could face legal consequences.

Data Protection and Privacy norms can be followed as per Government guidelines.

Further, under the Information Technology (Intermediary Guidelines) Rules, 2011, (https://www.meity.gov.in/writereaddata/files/GSR314E_10511%281%29_0.pdf) since the said Government department that is providing social media facilities is an intermediary, it has to comply with the Information Technology (Intermediary Guidelines) Rules, 2011. Under Rule 3(4) of the said rules, the Government department shall act within thirty-six hours, on receiving a written complaint from an affected person, and where applicable, work with the user or owner of such information to disable such information that is in contravention of sub-rule(2).

8.0 Data & Information Security Governance

The Government's communication to citizens via social media should follow the same data retention policy as its communication through other electronic and non-electronic channels.

9.0 Provisions related to Personal Information & Security:

Under the Information Technology Act, 2000, the Central Government has enacted various rules and regulations, which affect social media. Some of the most important ones in this regard are as follows: The Information Technology (Reasonable Security

Practices and Procedures & Sensitive Personal Data or Information) Rules, 2011 define provisions for personal information & security and what constitutes sensitive personal data.

Further under the Information Technology (Intermediary Guidelines) Rules, 2011, since the said Government department that provides social media facilities is an intermediary, it has to comply with the Information Technology (Intermediary Guidelines) Rules, 2011.

10.0 Personal Use of Social Media:

Guidelines for Police personnel on use of their personal Social Media Accounts:

Police personnel, like many people today, engage in Social Media through Social networking sites, blogging, etc. While most of this engagement is proper, in some instances what is said or done by the employee on internet could be detrimental to the department and its mission. Therefore, Department personnel shall abide by the following when using social media.

- a. Department personnel are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of this department for which loyalty and confidentiality are important, impede the performance of duties, impair discipline and harmony among co-workers, or negatively affect the public perception of the department. Any expression shall be subject to the Police forces (Restriction of Rights), Act 1965 & any other Act/Rules in force including the Official Secret Act.
- b. Department personnel should keep in mind that the content that they post and the way they engage on social media sites would reflect their department.
- c. They must clearly identify themselves. Employees may identify themselves as representatives of the agency. Self-identification can include the acknowledgment in the user profile for work experience, job title, etc., by identifying oneself as an employee of an agency.
- d. Confidential information must not be divulged. Employees must take proper care not to purposefully or inadvertently disclose any information that is confidential or law enforcement sensitive. Employees will also honour the privacy rights of other employees by seeking their permission before writing about or displaying internal agency happenings that might be considered to be a breach of their privacy, besides official secrets.
- e. Their views should not be seen to represent “official view” unless authorised to do so.
- f. For any official work involving transmission of public records, they must use an e-mail identity connected to a server, located in India and for this purpose they may utilize the services of National Informatics Centre (NIC) or the state government approved network.

- g. Terms of Service: Social networking sites require that users, when they signup, agree to abide by a terms of service (TOS) document. Agency employees are responsible for reading, knowing, and complying with the TOS of the sites they use. For example, most TOS agreements prohibit users from giving false names or other false information.
- h. Copyright: Employees at all times have to comply with the law in regard to copyright. Posting of someone else's work without permission is not allowed (other than short quotes that comply with the "fair use" exceptions). Other relevant laws that need to be complied with include those related to libel and defamation of character.
- i. Productivity: Agency employees need to comply with the general agency Internet use policy and recognise that all time and effort spent on their personal site should be done in their personal time and should not interfere with their official duties. Department personnel are prohibited from the Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any race, any religion, or any protected class of individuals.
- j. Department personnel should be aware that they might be subject to civil or criminal litigation for violating the Information Technology Act, 2000, and other laws of the land.
- k. Department personnel should be aware of their privacy settings on social media sites.
- l. Department personnel should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the department.
- m. Reporting violations— any employee becoming aware of or having knowledge of a posting or of any website or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-upaction.
