



**GUIDELINES**  
**TO ENSURE DISCIPLINE ON THE USE OF SOCIAL MEDIA**  
**BY GOVERNMENT EMPLOYEES**

**(NPM Division, BPR&D)**

## CONTENTS

|                                                      |    |
|------------------------------------------------------|----|
| 1. Introduction .....                                | 3  |
| 1.1 Objective.....                                   | 3  |
| 1.2 Purpose .....                                    | 4  |
| 2. Institutional Framework.....                      | 4  |
| 2.1 Clear Policies and Guidelines .....              | 5  |
| 2.2 Training.....                                    | 6  |
| 2.2.1 General Principles - Do's .....                | 6  |
| 2.2.2 General Principles - Dont's.....               | 8  |
| 2.3 Accountability .....                             | 9  |
| 3. Guidelines for Retired Government Employees ..... | 10 |
| ANNEXURE 1 Regulations against Violations .....      | 11 |
| ANNEXURE 2 References .....                          | 14 |

Disclaimer: This document is not a substitute for existing manuals or guidelines available in the States /UTs. However, it may be taken as a reference document for the States/UTs to make their own sets of guidelines.

# **GUIDELINES TO ENSURE DISCIPLINE ON USE OF SOCIAL MEDIA BY GOVT. EMPLOYEES**

(In response to Recommendation No. 29 of DGsP/IGsP Conference 2023 – “An effective mechanism be made to ensure discipline on use of social media by Government employees as even personal views of official appeared to be that of government.”)

## **1. INTRODUCTION**

In today's fast-moving and technology-driven world, communication has become much more vital than ever before. Effective communication enables governments to co-opt citizens into the developmental and other governance processes, and make them active contributors in nation building.

Government agencies are expected to regularly communicate with various stakeholders. However, there have been fundamental shifts in the size, scope and nature of communication from all types of organizations, especially at individual level.

Every Government Official is perceived by the public as a face of the government, whether she/he is on duty or off duty. The activities and opinions of government employees therefore have the potential to be seen as the government's official views. The actions and statements of government employees on social media can impact public perception of the government. Hence any kind of frivolous, ill-informed or unauthorized comments even on one's personal social media account have the potential to cause great damage. Regulation helps maintain a professional image and prevents actions that could harm public trust.

Therefore the following guidelines are devised to ensure discipline on use of social media.

### **1.1 Objective:**

To create guidelines for an effective mechanism to ensure discipline on use of social media by Government employees.

## 1.2 Purpose:

- i. **Preventing Conflicts of Interest:** Government employees might use social media to promote personal views or engage in activities that could conflict with their official duties. These guidelines will help ensure that their personal opinions or activities don't undermine their professional responsibilities.
- ii. **Maintaining Confidentiality and Security:** Government employees often have access to sensitive or classified information. Unregulated social media use can risk the accidental or intentional disclosure of confidential information, leading to potential security breaches.
- iii. **Avoiding Misinformation:** Government employees might inadvertently or deliberately share misinformation or unverified information. Regulation helps ensure that the information being disseminated aligns with factual and verified sources, maintaining public trust.
- iv. **Protecting Public Image and Trust:** The actions and statements of government employees on social media can impact public perception of the government. Regulation helps maintain a professional image and prevents actions that could harm public trust and cause embarrassment to the Government.
- v. **Ensuring Professional Conduct:** Social media can sometimes blur the lines between personal and professional conduct. Regulations can help maintain professional behavior, prevent harassment, and ensure that interactions remain respectful and appropriate.
- vi. **Legal and Ethical Compliance:** Government employees are often bound by specific legal and ethical standards. Regulation helps ensure that their social media activity complies with these standards and the law.

## 2. INSTITUTIONAL FRAMEWORK

Various media platforms occupy an important position in communicating the intent and activities of the government organizations to the general public. Further, the media plays a major role in shaping the perceptions about and the image of the government.

However, communication of the official stance has become more challenging in the current era of quick and unverified dispersal of information/misinformation on multiple media platforms by unauthorized individual government employees. .

Hence, there is need for setting up of institutional mechanisms by the different government departments and States/UTs, which may be similar to what is proposed below. Such framework should consist of clear policies, curated training modules and a mechanism for accountability to ensure discipline on the use of social media.

## **2.1 Clear Policies and Guidelines:**

- i. To address the increased responsibility of media communication, every HOD office may have a Media Briefing Cell (MBC) headed by a senior officer.
- ii. It may be divided into two wings – one dealing with the Print & Electronic Media, and the other dealing with the Social Media.
- iii. The MBC may be authorized to create and implement clear guidelines for media communication, including on social media.
- iv. Only Designated Officials should be authorized to communicate with the media.
- v. Offices at the district level may also have MBCs. They may brief the press/media, to give the factual position with regard to non- controversial matters such as on matters related to important issues, good initiatives, law and order, etc.
- vi. Government employees may be sensitized that social media sites may contain links that can infect equipment with viruses which can potentially alter, destroy or steal data, and infect connected devices. Secured internet connections only should be used for uploading or downloading of content to or from social media websites.
- vii. Social Media sites and Peer-to-Peer communication platforms may be used by adversaries to elicit classified information. This enhances chances of unintentionally sharing of classified information by the government servants in the public domain, which may have the potential to impact departmental security.
- viii. Guidelines should be issued by the State DGPs to ensure that the disclosures by the police do not result in media trial that lead to prejudging of the accused (Hon'ble Supreme Court directions in Criminal Appeal No. 1255/1999).

## **2.2 Training:**

- i. Periodic training should be conducted for media briefing, crisis communication, and media interactions for the personnel deployed in the MBCs in order to improve their functioning and reduce the possibility of incorrect communication.
- ii. The training modules should include relevant legislations.
- iii. The designated spokesperson should be made aware of the changing media landscape, the role of social media and the importance of having collaborative relationships with the media organizations.
- iv. The MBC as a whole should be trained and equipped for disseminating accurate and verified information clearly and concisely to the media.
- v. Separate training should also be periodically conducted for employees/officials who are not part of MBCs, to make them aware of the relevant institutional guidelines and do's and don'ts pertaining to personal and official social media accounts.
- vi. Government officials should be encouraged to spread awareness of social media perils amongst their family members and close friends, as they could also possess sensitive information at times.

During training, the following Do's and Dont's may be disseminated to participants:

### **2.2.1 General Principles - Do's:**

- i. Every government organization/department should have an effective mechanism in place to ensure discipline on use of social media by govt. employees.
- ii. Only Designated Officials should use the relevant official platforms to disseminate any official information to public or media.
- iii. Government employees should be mindful when expressing their views on the department and government policies and should refrain from mixing 'facts' and 'opinions'.
- iv. No classified/sensitive information should be posted on the internet under any circumstances.
- v. Government employees on sensitive duties should not reveal their exact nature of work or place of work or any work related activities on social media

platforms. Location and geo-tagging features should be switched off by such employees while using social media.

- vi. Government employees should be mandated not to express opinions on government policies/schemes etc. even through their personal social media accounts or to make political or religious statements in any public forum.
- vii. Employees should manage their account site settings to enable review and approval/rejection of comments by other users before such comments are allowed to appear on their timelines.
- viii. In case some adverse comment is still posted on the personal /official account of an employee without his/her knowledge, the concerned should immediately bring this to the notice of his/her seniors.
- ix. In the above case a suitable rejoinder should be issued immediately.
- x. Achievements of the department should be projected as such, and not as the individual efforts or achievements of any one officer.
- xi. The government employee will be personally responsible for the content published by him on blogs, wikis, or any other platform or in any form of user-generated content.
- xii. Employees should remember that anything posted on electronic media, even y accident, cannot be redacted or deleted permanently. Anything, once posted, can always be retrieved.
- xiii. Apps banned by Government of India should not be used. (The list of Banned Apps can be referred on website of Ministry of Electronics and Information Technology).
- xiv. Government employees should adhere to the department's code of conduct and ethical standards while using social media. This includes treating all individuals with respect, refraining from discriminatory language or behaviour, and upholding the principles of integrity and professionalism.
- xv. Officers should refrain from engaging in unprofessional behaviour such as online arguments, sharing inappropriate content, or using offensive language on social media.
- xvi. Care should be taken regarding appearance, the clothes/uniform worn and language used on online platforms. They should be befitting the dignity and decorum that is attached with the individual's identity as a government servant.

- xvii. Police organizations should utilize social media effectively to address fake news and rumors.
- xviii. Maximum restraint and caution should be used while sharing information about any arrest, raid or investigation on social media as any information shared on social media by any authentic/authorised source will reach a wide audience within a short period of time. The briefings should be confined to the essential facts only.
- xix. Only Designated Officers should disseminate information to the media on law and order incidents and criminal investigations, including important detections, notable achievements of the police department, disasters and other relevant situations.
- xx. The Conduct Rules of all government services may be modified to include suitable provisions to ensure discipline in use of social media.

#### **2.2.2 General Principles - Dont's:**

- i. The media briefings should be held after proper preparation and collection of facts and not be rushed.
- ii. Incomplete or unconfirmed information about ongoing government activities, and personal views, opinions or speculations on the same should be avoided.
- iii. Casual communication with the media should be avoided in order to prevent unintentional leakage.
- iv. Government employees should be advised not to post personal information or activities on official social media platforms and vice versa. Govt. engagements should not be posted on personal handles.
- v. Information/ pictures/ reels, etc. regarding official inspections, sensitive visits etc. should not be uploaded on one's personal social media account and vice versa.
- vi. Government emblem, insignia, uniform etc. should not be used in personal posts.
- vii. Showcasing official machinery including vehicles, offices, residences, uniforms, etc. amounts to misuse of government paraphernalia for building personal image and should be avoided.
- viii. No media briefing or communication (official or unofficial) should be done for the personal glorification of any officer.

- ix. Differences of opinion (official or personal) between government servants should not be aired in the public domain or posted on any account.
- x. Especially during media briefings, and also otherwise, adverse comments about other Government Departments, social values, traditions and local customs, etc., should be avoided.
- xi. Care should be taken to avoid endorsement of commercial entities or activities.
- xii. The different Police officers associated with sensational cases should not brief the media separately, as this could result in different versions.
- xiii. Police officers should avoid sharing/posting information about any investigation process and future operations in any case, that may hamper the probe.
- xiv. Information ought not to be released which would portray the police as insensitive or vindictive or which would suggest the pre-judging of an issue.
- xv. Official emails should never be used for creating or maintaining social media accounts.

## **2.3 Accountability:**

- i. A Government servant participating in public media in other than official briefings shall at all times make it clear that the views expressed by him/her are his/her own and not those of the Government.
- ii. As and when instances of sharing personal views/opinions etc. by any member of the department, in any manner that seems to imply that they are the official stand come to notice, a suitable rejoinder should be issued by the department.
- iii. In more serious cases, the matter should be taken up at the appropriate levels for remedial/disciplinary action against the erring officials and their controlling officer, depending on the nature of the violation.
- iv. While briefing the media, the designated officers must keep in view the applicable provisions of the Official Secrets Act, 1923, Manual of Departmental Security Instructions (MODSI) 2022, National Information Security Policy and Guidelines (NISPG), 2019, relevant Conduct Rules for government employees and other rules which may be applicable.

- v. Any deviation by the govt. employees concerned from the guidelines issued by the HOD with regard to the communication with the media and online activities should be viewed seriously and suitable action should be taken.

Further details on regulations against violations may be seen at Annexure 1.

### **3. Guidelines for Retired Government Employees:**

- i. Retired government employees can often provide valuable overviews and information on government policies, procedures and various issues or situations, due to which they are frequently invited on various media platforms.
- ii. Further, they may also wish to express their opinions on their personal social media accounts.
- iii. Care must be taken by such officials/personnel to ensure that only correct and relevant information is shared to avoid spread of rumors or misinformation.
- iv. It is also important to avoid any comments on sensitive topics that may have potential repercussions, for example on the ongoing investigation, law and order situations, government decisions and image, etc.
- v. The gravity of the Official Secrets Act, 1923 may be kept in mind before disclosing sensitive information to which the officials/personnel may have been privy during their career.

\*\*\*

## **REGULATIONS AGAINST VIOLATIONS**

Since information security violations could have grave consequences on national security, the following provisions of law exist that could be invoked against Government servants for such violations. Every government servant is expected to understand and follow these Acts, Rules and Procedures in their activities on Social Media:

**I. Indian Official Secrets Act (IOSA)-1923.**

- i. Section 5: prohibits communication of classified information to unauthorized persons or organizations and also holds all government servants responsible for taking reasonable care of such information.

**II. Information Technology Act 2000 as amended by (Amendment) Rules- 2011:**

- i. Section 66 and 67: prohibits violation of privacy of individuals and publication of obscene material including child pornography etc.

**III. Central Civil Services (Conduct) Rules -1964**

- i. Rule 11: prohibits communication, directly or indirectly of any official document or its part to anyone who is not authorized.
- ii. Rule 8(3): A Government servant publishing a book or participating in a public media shall at all times make it clear that the views expressed by him are his own and not that of Government.
- iii. Rule 9: prohibits a Government servant from making a public utterance, communication or statement of fact or opinion that can have the effect of adverse criticism of any current or recent policy or action of the government or which is capable of embarrassing the relations between the central government, state government or government of any foreign State.

**IV. Central Secretariat Manual of Office Procedure-2015**

- i. Chapter X: elaborates procedure of document security and sets up norms for authorized communication of government information.

V. The All India Services (Conduct) Rules - 1968

- i. Rule 6(2), Connection with press or radio—Previous sanction of the Government shall not be required when the member of the service, in the bonafide discharge of his duties or otherwise, publishes a book or contributes to or participates in a public media.

*Provided that he shall observe the provisions of rules and at all times make it clear that the views expressed, are of his own and not those of the Government.*

- ii. Rule 7, Criticism of Government.—No member of the Service shall, in any radio broadcast or communication over any public media or in any document published anonymously, pseudonymously or in his own name or in the name of any other person or in any communication to the press or in any public utterance, make any statement of fact or opinion —

1. Which has the effect of an adverse criticism of any current or recent policy or action of the Central Government or a State Government; or
2. Which is capable of embarrassing the relations between the Central Government and any State Government; or
3. Which is capable of embarrassing the relations between the Central Government and the Government of any Foreign State:

Substituted vide Notification No.11017/27/93–AIS 7(III) dated 13.01.1995 (GSR No. 52 dt. 04.02.1995)

Inserted vide Notification No. 11017/27/93–AIS (III) dated 13.01.1995 (GSR No. 52 dt. 04.02.1995)

Provided that nothing in this rule shall apply to any statement made or views expressed by a member of the Service in his official capacity and in the due performance of the duties assigned to him.

(GOI Instructions: D.P. & A.R. letter No. 11017/9/75–AIS (III), dated the 2nd March, 1976, reproduced under Miscellaneous Executive Instructions at the end of these Rules)

Note: Section 2(1)(d) of Bharatiya Sakshya Adhiniyam 2023 gives a new definition of the word document which is compatible with the modern digital era. The new definition specifically includes electronic and digital records within the scope of the term document.

**REFERENCES:**

- a. The draft Manual on Media Briefing by Police Personnel, shared with CS-II Division, MHA on 21.03.2024 by the NPM Division, BPR&D.
- b. The All India Services (Conduct) Rules, 1968
- c. Central Civil Services (Conduct) Rules, 1964
- d. Central Secretariat Manual of Office Procedure-2015
- e. Information Technology Act 2000 as amended by (Amendment) Rules, 2011
- f. Indian Official Secrets Act, 1923
- g. Manual of Departmental Security Instructions (MODSI) 2022