Government of Jammu and Kashmir
General Administration Department
Civil Secretariat, Jammu

Subject: Guidelines on the usage of social media by Government Employees.

Government Order No. 1646 –GAD of 2017
D a t e d : 26 – 12 - 2017

Sanction is hereby accorded to the notification of the guidelines, forming annexure to this order, on the use of social media by Government Employees.

By order of the Government of Jammu and Kashmir.

Sd/-
(Khurshid Ahmad) IAS
Commissioner/Secretary to the Government

No. GAD/Mtg/RB-IV/43/2017 Dated: 26-12-2017

Copy to the:

1. All Financial Commissioners.
2. Principal Resident Commissioner, J&K Government, New Delhi.
3. Director General of Police, J&K.
4. Principal Secretary to the Goyernor.
5. All Principal Secretaries to Government.
6. Chief Electoral Officer, J&K.
7. Principal Secretary to the Chief Minister.
8. All Commissioner/Secretaries to Government.
9. All Deputy Commissioners.
10. Chairperson, J&K Special Tribunal.
11. Divisional Commissioner, Kashmir/Jammu.
12. All Heads of the Departments/Managing Directors
13. Secretary, J&K Public Service Commission.
14. Director Estates, J&K.
15. Director, Information, J&K.
16. Director Archives, Archaeology and Museums.
17. Secretary, J&K Legislative Assembly/Council.
18. Secretary, J&K Services Selection Board.
19. OSD with the Deputy Chief Minister.
20. General Manager, Government Press, Srinagar/Jammu.

21. Private Secretaries to all Cabinet Ministers/Ministers of State.
22. Private Secretary to Learned Advocate General, J&K.
23. Private Secretary to the Chief Secretary.
24. Private Secretary to Commissioner/Secretary to the Government, GAD.
25. PRO to Advisor to Hon'ble Chief Minister.
26. Government Order file/Stock file/incharge website.

26.12.2011

(Imteeaz Kacho)
Deputy Secretary to the Government

GUIDELINES ON THE USAGE OF SOCIAL MEDIA

BY THE GOVERNMENT EMPLOYEES

Contents

I.**INTRODUCTION:** 3

II.**DEFINITIONS:** 3

III.**FRAMEWORK OF THE POLICY:** 4

IV.**OBJECTIVE: NEED FOR GUIDELINES** 5

V.**SCOPE:** 6

VI.**ACCEPTABLE USE:** 7

VII.**EMPLOYEE CONDUCT:** 8

VIII.**CONTENT:** 9

IX.**SECURITY:** 10

X.**LEGAL ISSUES:** 12

XI.**OFFICIAL USE OF SOCIAL MEDIA:** 14

XII.**POLICY ENFORCEMENT:** 16

I. INTRODUCTION:

The advent of social media is transforming the way in which people connect with each other and the manner in which information is shared and distributed. It is different from traditional media such as print, radio and television in two significant ways – first, the amount of content that can be generated by the users themselves far exceeds the content generated by news/opinion makers and second, its "viral" ability for potential exponential spread of information and interlinking of the various social media platforms, thereby considerably reducing the control over spread of any such information.

This policy aims at providing guidance on the correct use of social media by Government employees, thereby putting a check on information flow on the social media that employees share with others which happens in a contemporaneous manner. In the context of Rule 13(3) of the J&K Government Employees (Conduct) Rules,1971, it has been considered necessary to issue guidelines for their strict adherence by the constituents of the Government.

II. DEFINITIONS:

a) "**Government**" means the Government of Jammu and Kashmir.

b) "**Government employee**" and "**Employee**" means any person appointed to any civil service or post in connection with the affairs of the State. A Government employee whose services are placed at the disposal of a company, corporation, organisation or a local authority by the Government, shall also be deemed to be a Government employee serving under the Government.

c) "**Social Media**" means social networking sites such as Facebook or micro-blogging sites such as Twitter. However, very broadly, social media shall include any web or mobile-based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content.

d) "**Social media content**" means and includes any material, documents, photographs, graphics and other information that is created, posted, distributed, or transmitted using social media internet sites or social media tools.

e) "**Law Enforcement Agencies**" means the department which shall be entrusted with the monitoring of the social media activity of the Government employees.

f) "**Department**" means the wing of the Government of Jammu & Kashmir to which the employee belongs.

III. FRAMEWORK OF THE POLICY:

This document provides a framework regarding the use of social media by the Government employees and detailed guidelines governing each element of the framework. These elements of the policy will help a Government employee to use social media in conformity with the applicable Conduct Rules and Civil Service Rules. Briefly, the elements of the framework and associated guidelines are given below:-

The framework comprises the following elements:



- **Objective-** the need for guidelines to use social media.
- **Scope -** social media platforms covered under the guidelines.
- **Acceptable use-** guidelines on how employees are expected to use social media.
- **Employee conduct** - expectations for employees' conduct on social media sites.
- **Content** - type of content which can be posted on social media and what needs to be avoided.
- **Security** - security guidelines.
- **Legal issues** - legal considerations, service and conduct rules.
- **Official use of social media-** procedures for creation, maintenance and destruction of social media accounts for official use.

IV. OBJECTIVE: NEED FOR GUIDELINES

The progressive increase in the use of social media among the Government employees and its consequent impact have made it necessary to notify these guidelines on the use and the type of information that can be shared by the user over various platforms. There have been incidents in which the employees have vented their work stress on the social media, thereby creating unwanted issues for the administration. Such acts lead to breach of discipline contrary to what is expected of Government employees in the course of maintaining a reasonable and decent conduct in their personal lives, thereby staying clear of any disgrace to their service(s). These guidelines have been framed to make a distinction between the professional and personal lives of Government employees and making them aware of the following:

- Employees need to know and adhere to the various rules and regulations that exist while using social media.
- Employees should be aware of the effect their actions may have on their image as well as that of their departments. The information that they post or publish may remain public for a long time.

- Employees should be aware that the law enforcement agencies will observe content and information made available by them through social media. They should use their best judgment in posting material that is neither inappropriate nor harmful to the State.

V. SCOPE:

The social media policy covers wide social media platforms which are currently in use and the detailed explanation of the various types covered under the policy is tabulated as under:

Platform	Description
Social Networking	Social Networking is an online service that enables its users to create virtual networks with like-minded people akin to social networks in real life. It often offers facilities such as chat, instant messaging, photo sharing, updates, etc. Currently, social networking sites are the most prominent version of social media. Facebook, with 800 million users, is one of the most well known social networking sites.
Blogs	Blogs are descriptive content pages created and maintained by individual users and may contain text, photos and links to other websites. The main interactive feature of blogs is the ability of readers to leave comments and the comment trail can be followed.
Micro-blogs	Microblogs are similar to blogs with a typical restriction of 140 characters or less which allows users to write and share content. Twitter is the most well known micro-blogging site.
Vlogs & Video sharing sites	Video-blogs or Vlogs are blogging sites that mainly use video as the main form of content supported by text. Youtube is the largest video sharing site.
Wikis	A wiki is a collaborative website that allows multiple users to create and update pages on particular or interlinked subjects. While single page is referred to as "wiki page" the entire related content on that topic is called "Wiki." Wikipedia is the pioneering site of this type of platform.

VI. ACCEPTABLE USE:

Acceptable use defines the use of social media by the Government employees which is permitted by this policy. The exercise of sound judgment and an awareness of the acceptable use will go a long way towards avoiding problems during the use of social media. The guidelines are as follows:

- **Use of title and email address:** Employees may use their official title and Department affiliation on their personal social media page for professional identification or biographic data as long as they do not create an impression that they are communicating in an official capacity. Employees should not use their Government/official email addresses when setting up personal social media accounts.
- **Communicating in personal capacity:** Employees must avoid stating, implying, or creating the impression that they are communicating in an official capacity on behalf of the department in their personal social media activities.
- **Work or department-related posts:** Employees must not post, comment or share public information on matters related to their work or the work of the department but must properly safeguard privileged, confidential, classified, privacy-protected and/or sensitive departmental information. Moreover, they shall not tweet, retweet or share any electronic transmission.
- **Online discussions:** Employees should not engage in discussion on the social media by way of tweets, status updates, posts or blogs which are political in nature or on contentious issues that are violative of the applicable Conduct Rules. Employees must not post, update, share or promote any status or post that may be contentious or has the potential to create governance or law and order issues or are seen to propogate anything which is anti-social, anti-national or illegal.
- **Discrimination and harassment:** Employees should not use social media to engage in harassing or discriminatory conduct towards other employees (or individuals or groups) based on their race, color, religion, national origin, sex, gender identity, age, disability (physical or mental), genetic information, status as a parent, sexual orientation, marital status and/or political affiliation.

- **Anonymous and pseudonymous postings:** Employees should take care not to engage in any activity on social media that they otherwise would not be permitted to engage in if their identity was known. The applicable rules and standards of conduct apply equally whether an employee uses social media anonymously (or using a pseudonym) or while being properly identified.

VII. EMPLOYEE CONDUCT:

The Government employees should remain aware that, even though there are new ways to connect with the world, existing policies, rules and regulations are still implicated when communicating on social media. They should also recognize that they have responsibilities under the applicable rules of professional conduct and should consult those rules when considering a particular communication. It is important to note that while vastly accelerating the speed of communication and greatly broadening the size of the audience, the advent of social media neither restricts nor expands the existing limitations on employees' speech. This policy may restrict the speech of its employees when employees are speaking on matters of public concern or when the Government's interest in maintaining law & order outweighs its employees' interest of freedom of speech.

It is also intended to educate and remind the employees about the limitations in their communications that is derived from their status as Government employee. While the focus of this policy is to provide guidance for communications made on social media, Government employees should recognize that the standards and rules of appropriate professional conduct enacted by the Government from time to time are not limited to conduct in office only but also includes internet or electronic communications but rather apply to any public communication, whether written or oral.

The following restrictions apply to the conduct of the employees and any violation may lead to departmental action:

- **Ethical standards:** Employees shall not engage in criminal, infamous, dishonest, immoral or notoriously disgraceful conduct or other conduct on social media prejudicial to the Government.

- **Misuse of position:** Employees shall not use their social media accounts for endorsement of any product, service or enterprise or for the private gain of friends, relatives or other acquaintances or their own. Also, the employees shall not use their accounts in a manner that could reasonably be construed to imply that the Government endorses or sanctions their personal activities.
- **Political activity:** The Government employees shall not use their personal social media accounts for any political activity or endorsing the posts or tweets or blogs of any political figure.
- **Internet trolling:** All employees on social media need to exhibit decent and reasonable behaviour and must not be part of trolling on social media i.e. not to sow discord on the internet by starting arguments or upsetting people, by posting inflammatory, extraneous or off-topic messages in an online community (such as a news-group, forum, chat room, or blog) with the intent of provoking readers into an emotional response or of otherwise disrupting normal, on-topic discussion.

VIII. CONTENT:

Considering that there is no privacy on social media, any unwanted material posted on it can remain alive for years together due to the capability of social media of making it viral. There is a need to make the employees aware about the type of content posting that should be avoided during their social media activity. The guidelines in this regard are enumerated below:

- Employees directly or indirectly will not publish, post or release any information on social media that is considered confidential or not public or any official document or any part thereof or information to any Government employee or any other person to whom he is not authorised to communicate such document or information.
- No Government employee through any post, tweet or otherwise discuss or criticise on social media any policy pursued or action taken by the Government nor shall he in any manner participate in any such discussion or criticism that takes place on social media pages/communities or on microblogs.

- No Government employee shall post, tweet or share content that is political or anti-secular and communal in nature or subscribe to pages, communities or twitter handles and blogs of such nature.
- No Government employee shall indulge in any activity on social media or permit any person dependent on him for maintenance or under his care or control to undertake any activity on social media which is, or tends directly or indirectly to be, subversive of Government as by law established in the Country or in the State.
- A Government employee may, for the purpose or removing misapprehensions, correcting mis-statements, and refuting disloyal and seditious propaganda, defend and explain to the public the policy of Government in his posts and tweets on social media.
- Government employees shall not post on social media content or display comments about co-workers or any individual that are vulgar, obscene, threatening, intimidating or that violate the conduct rules of employees.
- No Government employee shall post grievances pertaining to their work place on social media in the form of videos, posts, tweets or blogs or any other form but will follow the already established channel of complaint redressal existing in the departments.
- The Government employees shall not indulge in sharing the so-called give-aways and contests on the social media platforms which are actually scams in disguise and they could unknowingly spread malware or trick people into giving away sensitive data by sharing it on their profiles.

IX. SECURITY:

Social media is possibly the most vital sector of the internet but, being open and social, creates legitimate concerns about privacy and safety. Despite these justifiable security concerns about the web, some of the reasons a person's social media account is compromised are self-induced. The compromised social media account can be a source of important and confidential data being leaked. Therefore, in order to protect the social media accounts, the employees should always remain aware of the following threats and adhere to the precautions listed:

- **Identity theft:** There are many security issues that confront the usage of social media, identity theft being the most important among them. Identity thieves gather personal information from social media sites through the information that is provided by a user and his activity on the social media. In order to protect accounts from identity theft, the employees should take the following precautions, viz. use of a strong password always; being careful with status updates (should not reveal personal information) and not revealing the location.
- **Using Third party apps:** On the app stores of mobile phones, numerous mobile application softwares are available for downloading. The employees should take care in selecting the app to download as many have been found carrying malicious software. Some of the malwares are designed to reveal the user's private information to a third party, replicate itself on other devices and destroy user data. Also the apps require certain level of user permission. Therefore, it should be made sure that the employee knows what the app is viewing and sharing before agreeing to the terms.
- **Clicking on enticing ads:** The enticing ads on social media are also a source of viruses and malware which are a potential security threat and should not be clicked on.
- **Connecting with strangers**: The employees should be careful while accepting invitations on social media platforms as subversive elements are always trying to be friends with the Government employees to extract information. Any friend requests from strangers as well as duplicate requests should be ignored. Caution should also be taken when connecting with a celebrity's account as scammers, sometimes, pose as famous people.
- **Evaluating security settings:** Social media sites provide the option to restrict persons who have access to personal information. The employees can improve the security of their social media accounts by disabling most of the options and then re-opening them once they understand what the settings specifically mean to their account. This way the employees can optimise the settings according to their preferences before using the various social media platforms and be more secure.
- **Becoming over-confident:** One of the biggest threats to online security is over-confidence. Having a firewall and an antivirus installed in a computer does not mean

there is no threat to security. The employees should not live under the impression that they don't have anything worth hacking, thus need not to worry about security. The inter-connected nature of today's technology does not only put the user to risk but also the other people who are connected to them. To keep themselves and their information safe, the employees should pay careful attention to their online activity. They should avoid posting the following information:

- ✓ Travel plans
- ✓ Bank account information
- ✓ Full address and date of birth
- ✓ Children's names, school, and birth dates
- ✓ Location information, such as the name of the work place
- ✓ Daily schedule

- **Be sceptical:** The employees should not believe in all that they read online. There are many false posts or misleading information about different topics that is available online. Therefore, appropriate precautions should be taken to verify the authenticity of any information before sharing it on social media sites.
- **Keep softwares, particularly web browsers, up-to-date:** Employees should install the latest software updates so that attackers cannot take advantage of known problems or vulnerabilities. Almost all operating systems and softwares offer automatic updates. If this option is available, it is always recommendable to enable it.
- **Use an anti-virus –** An anti-virus software helps protect the computer against known viruses. Since the attackers are continually creating new viruses, it is important to keep the virus definitions upto-date. The employees should make sure to have the latest security software and web browser against online threats.

X. LEGAL ISSUES:

The easy access to social media on the go has caused people to invariably post information on social media without understanding its ramifications. A number of times, people post content on various social media sites like Facebook, Twitter, etc. on the spur of the moment or on an impulse without thinking it through.

Thus, it becomes important for the employees to remain aware of the rules and regulations that govern actions of social media users in general and conduct rules

which over-see the employees' conduct in personal and professional life. The important and relevant rules and regulations are enumerated below:

- **Constitution of India Article 19(2):** Article 19(2) of the Constitution of India which deals with the right to freedom of speech also imposes reasonable restrictions which is reproduced as under:

  "Nothing in sub clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence."

- **The Information Technology Act:** The Information Technology Act was enacted in the year 2000 which regulates, controls and deals with the issues arising out of information technology. The act categorically makes users liable, should they post any incriminating or illegal content or material on social media. The law recognises user, providing content on social media, to be a content service provider and network service provider. Hence, the law recognizes social media users as network service providers and, hence, intermediaries under the law.

  Section 66 A: Punishment for sending offensive messages through communication service, etc.(Introduced vide ITAA 2008):

  Any person who sends, by means of a computer resource or a communication device,-

  (a) any information that is grossly offensive or has menacing character; or

  (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

  (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.

- **The Jammu and Kashmir Government Employees (Conduct) Rules, 1971:** These rules are applicable to all the Government employees of the State of Jammu and Kashmir and give details on the conduct that is expected of the employees in their personal as well as professional life. The rules list out the activities that are not to be carried out by the employees and violation of the conduct rules can be punished under rule 30 of the Jammu and Kashmir Civil Services (Classification, Control and Appeal) Rules, 1956.
- **The Jammu and Kashmir Civil Services (Classification, Control and Appeal) Rules, 1956:**

Rule 30: Punishment

The following penalties may, for good and sufficient reason and as hereinafter provided, be imposed upon members of a service, namely

(i) Censure;

(ii) fine not exceeding one month's pay;

(iii) withholding of increments and/or promotion;

(iv) reduction to a lower post and/or a lower time-scale and/or to a lower stage in time-scale;

(v) recovery from pay of the whole or part of any pecuniary loss caused to Government by negligence or breach of orders;

(vi) Premature retirement on proportionate pension other than that specified in rule 226 (2) of Jammu and Kashmir Civil Service Regulations.

(vii) removal from the service of the State which does not disqualify from future employment;

(viii) dismissal from the service of the State which ordinarily disqualifies from future employment.

XI. OFFICIAL USE OF SOCIAL MEDIA:

There has been an increasing trend among the Government functionaries of creating social media pages of their departments or of the office they hold, which disseminates official information with regard to public services. The objective for the official use of social media should not be just to disseminate information but also to

undertake public engagement for a meaningful public participation for formulation of positive public opinion. Government organisations should explore the use of social media for disseminating information, policy making, generating awareness, education, etc. about public services. Lack of a clearly defined policy on account management enables situations where accounts are established on behalf of departments without executive knowledge and organizational approval. The guidelines for creation, maintenance and destruction of social media accounts for official use are as under:

- **Account creation:** The social media accounts for official use should be opened in the name of the department or designation under proper formal orders which states:
  - ✓ The name under which account is opened with official email id.
  - ✓ List of employees having access to official account
  - ✓ Who will hold password for the account
  - ✓ Scope and content to be posted
  - ✓ Record keeping guidelines
- **Response:** The responses on the official social media pages/accounts shall adhere to the following guidelines–
  - ✓ Not all posts/comments need to be responded to immediately and individually. Also, wherever a response is required, all posts should be kept short and to the point.
  - ✓ There has to be a defined hierarchy not only of responses but also of queries. For example, the comments and queries may be classified as routine – for which a Frequently Asked Question (FAQ) and Fixed Response Format (FRF) may be applied.
  - ✓ The next level of query/comment may be more specific where an "official" response may be needed. Such a categorization will help organizations in streamlining their responses.
  - ✓ There should be congruence between responses posted on social media and those in traditional media.
- **Records management:** It shall be necessary for departments maintaining the account to keep record of the information shared or guidance given online. All relevant records should be captured, trail generated and records managed

appropriately. The following guidelines need to be adhered to while maintaining records:

- ✓ No record may be maintained of queries on the social media account which do not require any decision making or influence any Government policy.
- ✓ Consultations which are undertaken on specific policy or governance issues or that may involve decision making, should all be recorded by way of screen shots or in any other manner.
- ✓ A summary may be created of the information/consultation on the social media account and filed.

- **Moderation:** A moderation policy should also be published in the 'About' section of the page for others to add their own content. This informs people about what they can post on the official page.
- **Destruction of official account:** Like creation of account, the destruction of the account if there is poor public response should be put on record through a formal order so that any false account by the official name could be detected later on.

XII. POLICY ENFORCEMENT:

- The Government shall monitor the social media to track violations of the guidelines and shall maintain official records of violations that contain certain data related to social media activity of Government employees.

- Therefore, Government Employees should adhere to the above guidelines to ensure against disciplinary action and consequent punishment which will be as per the Jammu and Kashmir Civil Services (Classification, Control and Appeal) Rules, 1956 and largely depend upon the nature and severity of the violation.

- In case the violation of the guidelines involves an offence under law, it will attract necessary legal action.