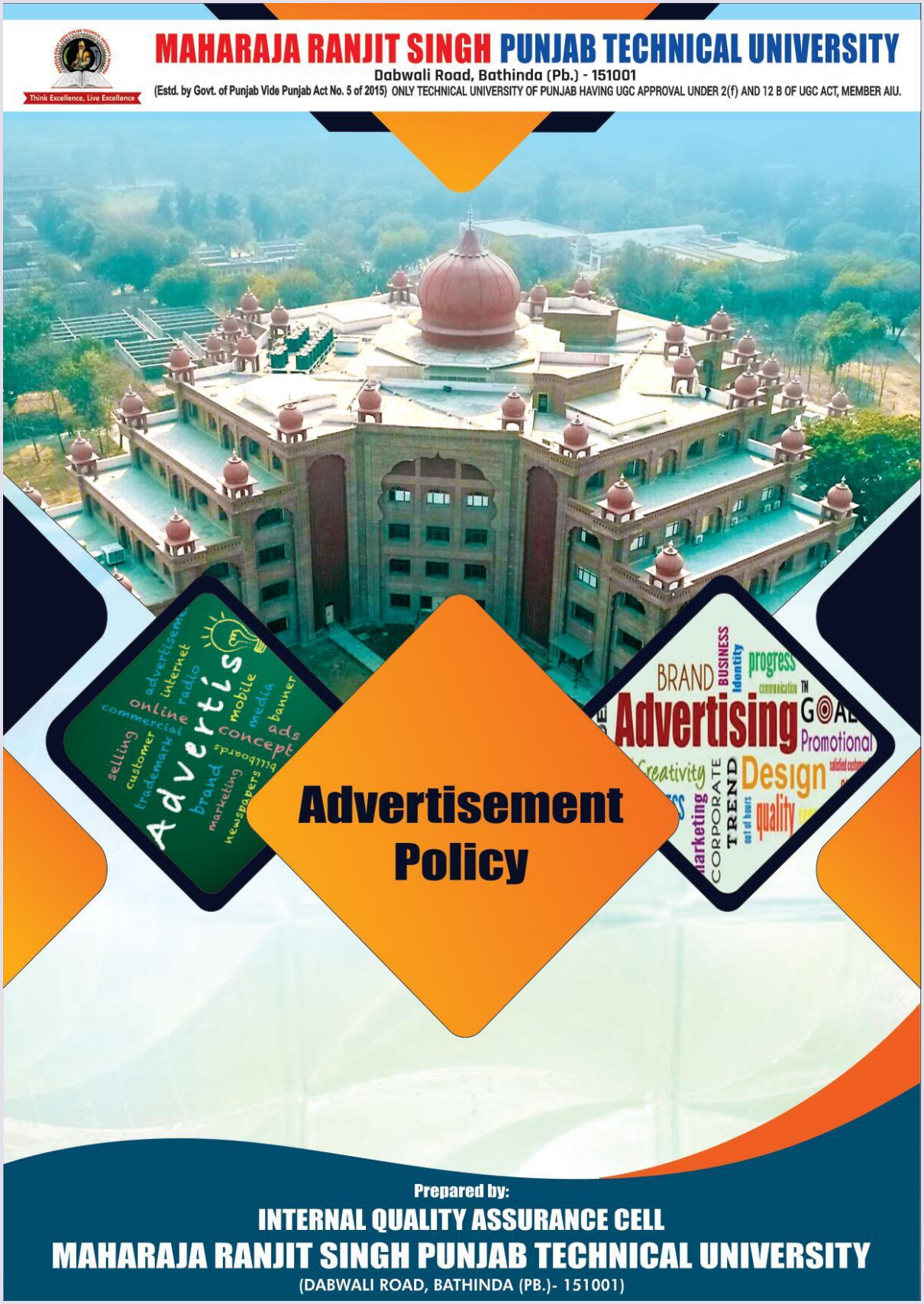

MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
Dabwali Road, Bathinda (Pb.) - 151001
(Estd. by Govt. of Punjab Vide Punjab Act No. 5 of 2015) ONLY TECHNICAL UNIVERSITY OF PUNJAB HAVING UGC APPROVAL UNDER 2(f) AND 12 B OF UGC ACT, MEMBER AIU.
Think Excellence, Live Excellence
Social
Media
Policy
You
Tube
Prepared by:
INTERNAL QUALITY ASSURANCE CELL
MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
(DABWALI ROAD, BATHINDA (PB.)- 151001)


MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
Dabwali Road, Bathinda (Pb.) - 151001
(Estd. by Govt. of Punjab Vide Punjab Act No. 5 of 2015) ONLY TECHNICAL UNIVERSITY OF PUNJAB HAVING UGC APPROVAL UNDER 2(f) AND 12 B OF UGC ACT, MEMBER AIU.
Think Excellence, Live Excellence
Advertisement Policy
Prepared by:
INTERNAL QUALITY ASSURANCE CELL
MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
(DABWALI ROAD, BATHINDA (PB.)- 151001)

SOCIAL MEDIA POLICY

2021

INTERNAL QUALITY ASSURANCE CELL

MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
BATHINDA 151001

SOCIAL MEDIA POLICY

Prepared by

- Mr. Harjinder Sidhu, Director, PRO, MRSPTU.
- Mr. Harjot Singh Sidhu, T&P, MRSPTU.
- Mr. Rahul Garg, ITeS, MRSPTU.

Inputs by

- Dr. Ashish Baldi, Director, IQAC

Version 1

Year 2021

INTERNAL QUALITY ASSURANCE CELL

Social Media Policy

Social Media Guidelines for Students & Staff Members

This set of social media guidelines aims to set standards that are expected of all students and staff members with respect to the responsible use of social media, prevention of harassment and promotion of harmony in the online space.

1. Every bonafide student and staff members of MRSPTU should be mindful that information shared on social media becomes public information and hence should not use social media in any way that may compromise your reputation or professional practice at a later stage. Any adverse content that goes against the rules of MRSPTU, the Constitution of India and does not promote general harmony could be brought to the attention of the University, future employers and / or professional bodies and may be detrimental to studies and / or future career.
2. Any content maligning MRSPTU, its policies and employees will be viewed adversely inviting disciplinary action and inter alia, penalties, debarment from sitting the examination, campus placements etc.
3. No student/ staff member may claim to speak on behalf of, or represent, the University on social media websites without the University's prior permission. You should not declare, imply or indicate that the content of any social media site under your control is representative of the University. When posting online there may be circumstances in which the student/ staff member gives the impression that he/she is speaking on behalf of the University or department. Students/ staff member should consider adding a disclaimer to make it clear that they are posting in personal capacities.
4. Social media (for example; Twitter, Facebook; Google+; LinkedIn; Instagram; and open forums and Blogs) are now a common feature of everyday life, enabling and supporting both students and staff in academic and collaborative opportunities. Any form of harassment, including on social media platforms, is unacceptable and will be treated very seriously by the University inviting disciplinary proceedings.
5. Every student/ staff member should respect individual rights to privacy and have regard for the feelings of others. They must not disclose personal details, including pictures, of other students or staff without their prior permission.

6. Students/ staff member should be mindful of the enduring nature of information posted on social media sites and should be careful while writing posts or sharing information.
7. Using social media to post offensive comments, images or other content is a breach of the Code of Discipline under Rules & Regulations of the University and will result in disciplinary action and also liable for legal action as per the provisions in IT Act 2000 & Amendments 2008.
8. Civil and criminal laws apply to content posted online. Civil claims that could be brought include actions for defamation, harassment, breach of intellectual property rights, fraudulent misrepresentation or breach of confidence. Criminal offences that could occur online include harassment, stalking, hate crimes, coercive or controlling behaviour, disclosing intimate images without consent, blackmail, malicious communications and terrorism offences. Cyber laws as are applicable in the Indian Territory will be applicable to contents posted online.
9. Posting others' content online (photographs, text, videos, music etc.) without prior and proper permission to do so, including specific terms of any licence – for example, credit the author and/or link to the licence, revealing trade secrets, violations of IPR et al will be viewed adversely and liable for legal action among other things.
10. The University is not responsible for, and does not hold any ownership of, any content posted on social media by its students.
11. Usage of MRSPTU brand trademark/service mark without prior written permission is liable for legal action.
12. It is mandatory for every student at the time of admission to sign an undertaking on social media usage along with anti-ragging and other such formalities.

Online Etiquette

When using social media it can be tempting to speak and act in a way we wouldn't when we are face-to-face. Remember that innocuous comments posted online may be misconstrued, as the written word has permanence/ taken screen shots of/ lack the nuances of face-to-face interaction.

Ask yourself these questions:

- Who'll be reading my post?

  Will it be limited to close friends and family or could it be read by the wider public? Could it be seen by people you have, or might one day have, a professional relationship with?

  If there is an issue concerning the campus/friends/classmates/ faculty, have it escalated it at the appropriate forum for redressal. Posting problems on social media is not a solution and only makes things worse.

- What style should I be using?

  Always be courteous, even when you don't feel like it. Remember that it in most cases, the content you post will be public and it may not be possible to remove it at a later date. It could be reposted or shared through other forms of social media.

- Think twice about how you post content if you're feeling angry about something and consider the effect that this might have on the situation. If you're responding to someone else's post ask yourself whether you are sure that you have read the post in the way in which it was intended.

SOCIAL MEDIA POLICY

Department of Electronics and Information Technology

Framework & Guidelines for Use of Social Media for Government Organisations

Department of Electronics and InformationTechnology Ministry of Communications &

Information Technology Government ofIndia

Table of Contents

Executive Summary

Information Communication Technologies (ICTs) including internet and mobile based communications are increasingly becoming pervasive and integral to day-to-day functioning of our lives- whether personal or official. ICTs offer an unprecedented opportunity of connecting to each and every individual and design the communication structure accordingly to each person. Such a structure can be defined and re-defined by both initiator and receiver of communication. Such a medium of communication is referred to as Social Media and it is transforming the way in which people connect with each other and the manner in which information is shared and distributed.

While at a personal level, the uptake and usage of such media is gaining rapid popularity, use and utility of such media for official purpose remain ambiguous. Many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated. These guidelines will enable the various agencies to create and implement their own strategy for the use of social media. The document will help them to make an informed choice about the objective, platforms, resources, etc. to meet the requirement of interaction with their varied stakeholders.

The guidelines provide an in depth review of types of social media, their characteristics and challenges in their uses. In order to assist the departments to undertake such an engagement, the document provides for a framework and detailed guidelines governing each element of the framework. Briefly, the elements of the framework and associated guidelines are given below:

The framework comprises of the following 6 elements:

- Objective: Why an agency needs to use social media
- Platform: Which platform/s to use for interaction
- Governance: What are rules of engagement
- Communication Strategy: How to interact

- Pilot: How to create and sustain a community
- Institutionalization: How to embed social media in organization structure Some of key caveats that the guidelines highlight and must be kept in mind include:
- All accounts must be created and operated in official capacity only
- As social media demands 24*7 interactions, some responsiveness criteria may be defined and a dedicated team may be put in place to monitor and respond
- There should be congruence between responses on social media and traditional media
- Relevant provisions of IT Act 2000 and RTI Act must be adhered to.

Detailed description and explanations are given in the Guidelines section of the document.

Social Media is being used across the world by different government agencies. The document also illustrates some examples from India as well from other countries to demonstrate the purpose and use of such media. It is believed that the Framework and Guidelines will be useful for departments and agencies in formulating their own strategies and will help them in engaging in a more fruitful manner with their respective stakeholders.

Guidelines for Use of Social Media by Government

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 by word of mouth and interlinking of the various social media platforms, thereby considerably reducing the control over spread of any such information. These characteristics denote the paradigm shift from Web 1.0 technologies that enabled simple information sharing and basic two-way transactions to Web 2.0 – where literally everyone is/can be a user as well as generator of content. Social media is redefining the way people communicate with one another.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated. These guidelines will enable the various agencies to create and implement their own strategy for the use of social media. The document will help them to make an informed choice about the objective, platforms, resources, etc. to meet the requirement of interaction with their varied stakeholders.

II. Need for Social Media Guidelines

Given its characteristics to potentially give "voice to all", immediate outreach and 24*7 engagement, Social Media offers a unique opportunity to governments to engage with their stakeholders especially citizens in real time to make policy making citizen centric. Many governments across the world as well many government agencies in India are using various social media platforms to reach out to citizens, businesses and experts to seek inputs into policy making, get feedback on service delivery, create community based programmes etc.

However, many apprehensions remain including, but not limited to issues related to authorization to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc.

It was therefore felt that Guidelines for use of Social Media were required which would enable project owners/implementers to effectively use these platforms.

III. Target Audience

The Framework and Guidelines have been developed for MRSPTU help them conceptualise and evolve their Social Media interactions and strategy.

IV. Social Media

4.1 What is Social Media

Social Media in recent times has become synonymous with Social Networking sites such as FaceBook or MicroBlogging sites such as Twitter. However, very broadly social media can be defined as any web or mobile based platform that enables an individual or agency to communicate interactively and enables exchange of user generated content.

4.1.1. Social Media Characteristics

Critical characteristics of social media are

- **Connectedness:** This attribute showcases the media's ability to connect and re- connect like-minded people or people interested in same topics and domains. Through this media, 24*7 connectedness is possible through a variety of media and access devices including PCs, Laptops, mobile phones etc. Individuals re-tweeting & following other people's comments and status and updating their own account at all hours are examples of this attribute.
- **Collaboration:** The connections achieved on this media, enable people to collaborate and create knowledge. Such collaborations can be either open or closed. Wikipedia is an example of open collaboration which enabled creation of an open web based encyclopedia through contribution from hundreds of thousands of people. GovLoop is an example of closed collaboration wherein experts groups contribute on specific policy matters.
- **Community:** Connectedness and collaboration helps create and sustain communities. These communities can create awareness about various issues and can be

used for seeking inputs into policy making, building goodwill or even seeking feedback into delivery of publicservices.

Pictorially, the characteristics have been depicted below to show the inter-linkages between all characteristics and their mutual dependency.

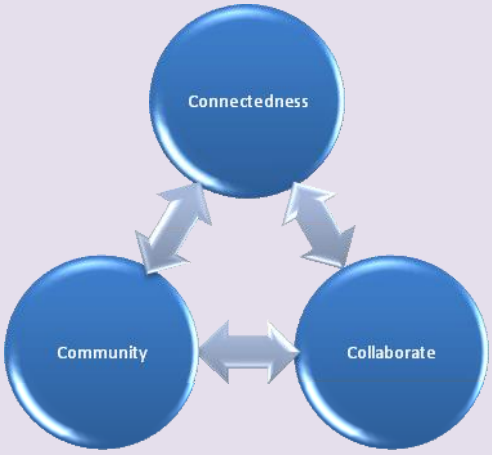


Figure 1: Characteristics of Social Media

4.2 Need for Using Social Media

With the ever increasing diffusion of ICTs in all walks of lives, connectedness is increasingly becoming a given part of our lives. This connectedness brings with it many opportunities and also presents many challenges. From the perspective of University, the following represent some of the reasons for using social media:

- **Enhanced Outreach**: As the recent world events have demonstrated, social media have emerged as a powerful platform for forming an opinion as well as generating mass support. In India, FaceBook alone has over 40 million users each. Even a microblogging site Twitter has about 16 million users. These sites offer an opportunity to reach out this audience at a key stroke. Many of these facilitate access through mobile devices and with nearly 900 million mobile users in India, it offers an unprecedented outreach.
- **Real Time engagement**: Social Media releases the shackles of time and place for engagement. They can connect policy makers to stakeholders in real time.
- **Individual Interaction**: In tradition forms of media, interaction with individual user is either not possible or is very limited. Social Media platform offers the ability to connect with each and every individual. Such an interaction also enables the marginalised to participate in

discussions and present their point of view, thereby improving the political position of marginalized or vulnerable groups. It is specifically useful when seeking feedback on services rendered.

- **Managing Perceptions**: One of the big challenges for government is to avoid propagation of unverified facts and frivolous misleading rumours with respect to government policies. Leveraging these platforms can help to counter such perceptions and present the facts to enable informed opinion making.

4.3 Types of Social Media

Kaplan and Haenlein in 2010 classified social media into six different types: collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. A brief description of some of the most common types of social media is given below:

Platform Type	Description
Social Networking	Social Networking is an online service that enables its users to create virtual networks with likeminded people akin to social networks in real life. It often offers the 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 site.
Blogs	Blogs are descriptive content pages created and maintained by individual users and may contain text, photos and links to other web sites. The main interactive feature of Blogs is the ability of readers to leave comments and the comment trail can be followed.
MicroBlogs	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 microblogging site.
Vlogs and 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
	a "Wiki". Wikipedia is the pioneering site of this type of platform.

Table 1: Types of Social Media

A more detailed description of the different types of social media, their characteristics is given in **Annexure-I**

4.4 Core Values for Using Social Media

Unlike other traditional media, social media is more interactive, enables one-to-one conversation and demands immediacy in response. Also, on such platforms the perception of official and personal roles and boundaries is often blurred. Therefore, while using social media for official purposes, the following may be kept in mind to smoothen interaction:

- **Identity**: Always identify clearly who you are, what is your role in the department and publish in the first person. Disclaimer may be used when appropriate
- **Authority**: Do not comment and respond unless authorized to do so especially in the matters that are sub-judice, draft legislations or relating to other individuals
- **Relevance**: Comment on issues relevant to your area and make relevant and pertinent comments. This will make conversation productive and help take it to its logical conclusion.
- **Professionalism**: Be Polite, Be Discrete and Be Respectful to all and do not make personal comments for or against any individuals or agencies. Also, professional discussions should not be politicized.
- **Openness**: Be open to comments – whether positive or negative. It is NOT necessary to respond to each and every comment
- **Compliance**: Be compliant to relevant rules and regulations. Do not infringe upon IPR, copyright of others
- **Privacy**: Do not reveal personal information about other individuals as well as do not publish your own private and personal details unless you wish for them to be made public to be used by others.

4.5 Challenges in Using Social Media

a) **Why to use social media:** Departments sometimes find it difficult to define the need or objective to use social media. Is it for providing information, seeking feedback, generic interaction, etc. Due to this lack of clarity, departments often either choose not to use social media or attempt to be present on all platforms at once.

b) **Which Platforms to use:** Given the plethora of platforms and even types of social media, it is very difficult to choose the type and no. of platform on which to engage and how to create inter-linkages between these platforms.

c) **Who will engage**: Most departments have limited capacity to engage with traditional media itself and since social media demands a deeper and constant interaction, availability of such resources is even more limited. A closely associated question is that of authority i.e. who is authorized to respond on behalf of the department, whether such

a response will be made in personal or official capacity and from personal or official account etc.

d) **How to engage**: Use of social media is an ongoing process and requires long term commitment. Many have questions around rules of engagement – how to create and manage an account, what should be response time, what are the legal implications etc.

In order to help departments and government agencies to meet these challenges, Guidelines for use of Social Media have been drafted. In the following section, various elements of the Framework and the Guidelines to use the different elements of Framework have been detailed.

V. Social Media Framework & Guidelines for Government Organisations

The Social Media Framework for the Government of India has been created to enable government agencies to use these platforms more effectively and reach out to their stakeholders and understand their concerns and hear their voices. The Framework comprises of the following 6 elements:

- **Objective**: Why an agency needs to use social media
- **Platform**: Which platform/s to use for interaction
- **Governance**: What are rules of engagement
- **Communication Strategy**: How to interact

- **Pilot**: How to create and sustain a community
- **Engagement Analysis**: Who is talking about what, where and what are the main points of conversations
- **Institutionalisation**: How to embed social media in organisation structure

Pictorially the framework can be represented as given below:

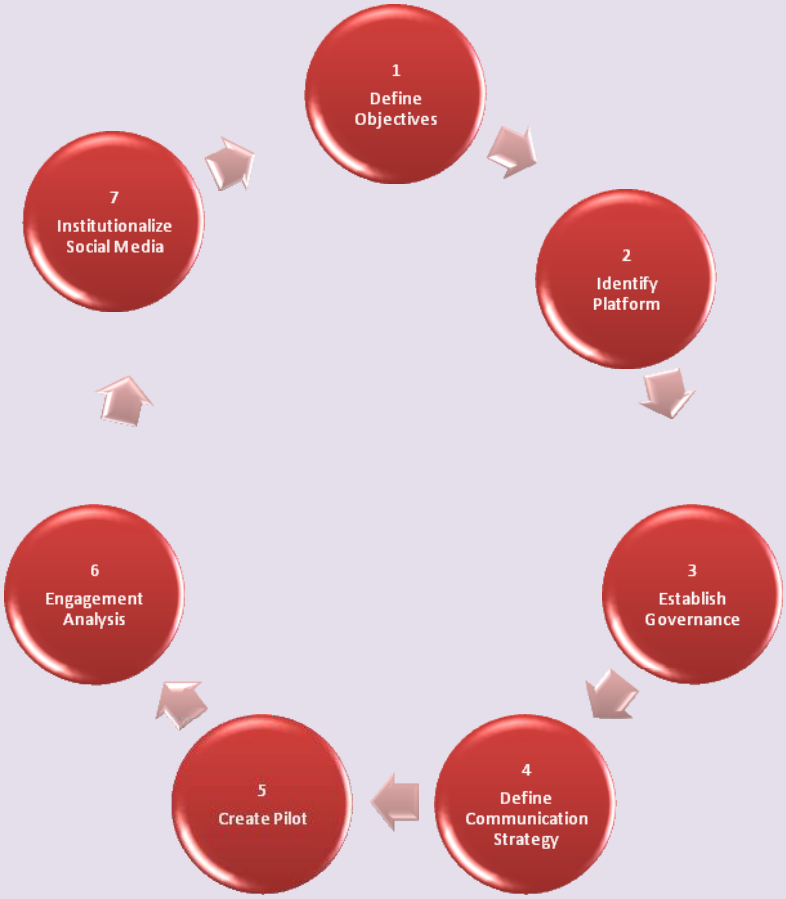


Figure 2: Social Media Framework

(Adapted from http://www.rossdawsonblog.com/SocialMediaStrategyFrameworkv1.pdf)

The next section elaborates on each element and provides guidelines on important aspects and caveats of each element. The guidelines also use examples from India and across the world to illustrate each element.

5.1. Guidelines for Using Social Media by Government Organizations

This section provides the users in government organizations, a set of guiding principles that may be used while making use of Social Media. The section will illustrate through appropriate examples, some of the critical aspects of each element.

5.1.1 Define Objectives

The objective for the use of social media is not just to disseminate information but also to undertake public engagement for a meaningful public participation for formulation of public policy. Government organisations are exploring the use of social media for public engagements for disseminating information, policy making, recruitment, generating awareness, education etc. about public services. Therefore, Social Media may be used for:

- Seeking feedback from citizens
- Re-pronouncement of Public Policy
- Issue based as well as Generic interaction
- Brand Building or Public Relations
- Generating Awareness and education on National Action Plans and implementation strategies

In the Indian context, care must be taken so that people can communicate in their own language, and due cognizance of the views expressed in local languages is taken.

5.1.2 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 other forms of social media include, Social bookmarking site – stumble upon; transaction based platforms – Amazon & eBay; self-publishing media – You Tube, Picasa; Business management etc. Since the choices are many, it is essential to identify one or two key platforms from which the department may begin interaction. Based on objective and response, the basket of platforms may be enhanced.

Government departments and agencies can engage social media in any of the following manner:

- By making use of any of the existing external platforms, or
- By creating their own communication platforms
- The choice of the platform – whether owned or externally leveraged should be made based on the following factors:
- Duration of engagement - whether the engagement sought is to be an ongoing activity or created for a specific time-bound purpose

- Type of Consultation – whether the consultation is open to public or confined to a particular group of stakeholders e.g. experts
- Scope of Engagement – whether the consultation requires daily, weekly, bi-weekly or even hourly interaction
- Existing Laws – whether existing laws permit use of such platforms and the requirement under such laws regarding data protection, security, privacy, archiving etc.

5.1.3 Governance Structure:

Since use of social media is a 24*7 engagement, the extant rules and regulations of media interaction do not fully apply to them.

Two most important aspects of social media are its:

- Viral characteristic – news spreads exponentially; and
- Demand for instant gratification – queries, responses and counter-responses are posted instantaneously.

However, since the official pages of departments must reflect the official position, some measure of control must be included in the flexible design of communication.

Just as rules and regulations exist for interaction with traditional media, similar rules must be created for engaging with social media.

Some of the key aspects of such a governance structure include:

5.1.3.1. Account Governance

Account Creation: A social media account establishes an organisation's online identity. Wherever possible, the same name for the different social networking accounts may be adopted to ensure ease of search on the internet. Another important facet of online identity is the need for it to be rendered effectively in either long form e.g. website address or in 15 characters or less (this is the Twitter maximum).

Login and passwords: 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.

Account Status: It is important to define whether the engagement may be undertaken through official accounts only or the officials may be 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.

5.1.3.2. Response and Responsiveness:

Responsiveness: This indicates the 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 the some kind of response within a pre-defined time limit.

As far as possible, it is important to state upfront the scope of response – given/not given, type of response – official/unofficial, response time – 1 day/1 week etc. so that expectations are set correctly. Some of the ways to ensure timely response is Email integration i.e. email writing, list management, list building, proper lead direction so the right internal person takes actions on leads in a timely fashion and Daily management/maintenance of social media platform messages, customer contacts, etc.

Response*:* While creating a policy for responses, it may be noted that -

- 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.
- 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.
- Another important aspect that needs to be addressed is the Escalation Mechanism.
  - 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 may be queries/comments related to projects/programme, for which no separate official response may be needed because all relevant information may be available in the public domain and the query may be responded accordingly.
  - 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.

- Finally, there should be congruence between responses posted on social media and those in traditional media.

5.1.3.3. Resource Governance

Allocation of Resources: 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. Many organizations have a dedicated team including outsourced resources to manage their engagement while others primarily uses internal resources. More often than not, it is advisable to create a dedicated team. One of the key issues that impacts the resource requirement is whether the conversation is moderated or un-moderated. In case of moderated conversation, dedicated resource/s is critical. 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 in social media requires different skill sets, the champion and other resources identified would require orientation & training specifically for the tasks assigned to them and keep abreast of the fast paced developments in this media

Roles & Responsibilities: The roles and responsibilities of the team responsible for creating, managing and responding on social media platforms must be clearly defined.

- In Indian context, they may also need to be aligned to roles and responsibilities defined for responding to RTIs.
- For most interactions, flexibility may be given to the staff to respond to regular queries or comments.
- Escalation mechanism defined in the governance structure must clearly define accountability at all levels.
- The role definition 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. For example, while the existing web content team may be assigned the responsibility for responding to usual queries; special technical expertise may be required to ensure appropriate levels of security.

Accountability: Clearance systems that distinguish between situations when an official position is required, and when open conversation is appropriate. This has to have at its heart a redefinition of accountability. 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 Amendment Act 2008.

Content Governance:

Content Creation & Social media profiles overlap, therefore sharing consistent content on all social media platforms should form the bedrock of content policy. While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.

Accessibility: In order to enable wider participation, content creation and availability should be in Indian languages and must not be limited to text alone. The content should follow the Government of India Guidelines for Website and adequately address challenges related to accessibility in Indian Languages as well as accessibility of content for differently abled.

Moderation*:* 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 matter related to copyright, rights to addition and deletion etc.

Records Management: When any information is shared or guidance given online, it is necessary to ensure that all relevant records are captured, trail is generated and records are managed appropriately. It is important that the rules regarding record keeping are states upfront so that those seeking historical data are aware of statutes and limitations. Some of the important aspects that may be kept in mind while defining record management guidelines are as under:

- The requirements for existing legislations e.g. RTI etc. need to be kept in mind and are paramount in influencing decisions regarding record keeping
- Ordinarily, if online consultations do not impact decision making, lead to or influence policy making (e.g. seeking information about nodal officers, or any other public document, or responding to generic comments such as governance should be improved etc.) the agencies may decide that no record of such interactions will be maintained.
- However, if consultations are necessarily being undertaken on specific policy or governance issues or that may influence decision making (e.g. inputs into Plan Document, consultation on policy frameworks etc.) then all necessary records need to be maintained. If the agency is using a social media site that does not facilitate record keeping, then there are various other options that may be explored. Some of the options are given below and may

be exercised based on need and resources available:

- Records may be created agency's internal platform and records be 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 Since most of the social media platforms are based outside India and are not governed by Indian Laws, or managed and controlled by Indian regulations, specific policies may be drafted related to information security and archiving. If required the agencies may engage with the Social Media Service Providers to work out Service Level Agreements for

- Complaint and response mechanism between the agency and the Service Provider
- Content Storage
- Shared access of the content
- Archival mechanisms

5.1.3.4. Legal Provisions: In India, the legal implications must be viewed in accordance with the law of land e.g. RTI Act, IT ACT 2000 & IT Amendment Act 2008 etc as also rules and regulations made thereunder. These policies must be circulated internally to ensure uniformity of response. Some of the key sections and their implications that must be kept in mind are as under:

5.1.3.4.1. When 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. The said conditions which need to mandatorily

complied with the Government department to claim exemption for any third party data information or communication link made available or hosted by them in connection with social media facilities made available by the said department on their network are as follows:

- The function of the Government department is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted
- The Government department does not-
  (i) Initiate the transmission,
  (ii) Select the receiver of the transmission, and
  (iii) Select or modify the information contained in the transmission
  - The Government department observes due diligence while discharging its duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
  - That the Government department as intermediary must not conspire or abet or aide or induce, whether by threats or promise or otherwise in the commission of the unlawful act.
  - That the Government department must immediately after receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the Government department is being used to commit the unlawful act, must expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
  - The Government department must also comply with all applicable rules, regulations and notifications in regard to their activity of providing social media facilities on its network.
  - That the Government department complies with the Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011.
  - That the Government department also complies with the Information Technology (Intermediary guidelines) Rules, 2011.

- That the Government department also implement reasonable security practices and procedures as envisaged under Section 43A of the amended Information Technology Act, 2000.

5.1.3.5. 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. Data portability compliance varies from one social media platform to another. Hence, privileged access may be mandated by the Government along the same lines "take down notices" and "information requests" currently being sent to social media and other platforms for intellectual property rights infringement and other offences.

Provisions related to Personal Information & Security: Under the Information Technology Act 2000, the Central Government has enacted various rules and regulations which impact social media. Some of the most important in this regard are as follows:

i. 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. Sensitive personal data or information of a person means such personal information which consists of information relating to;—

a. Password;
b. Financial information such as Bank account or credit card or debit card or other payment instrument details;
c. Physical, physiological and mental health condition;
d. Sexual orientation;
e. Medical records and history;
f. Biometric information;
g. Any detail relating to the above clauses as provided to body corporate for providing service; and
h. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these

rules.

ii. For the purposes of protecting such sensitive personal data, the Government has mandated that any legal entity who is processing, dealing or handling sensitive personal data must implement reasonable security practices and procedures.

iii. 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.

iv. Further under the Information Technology (Intermediary guidelines) Rules, 2011, since the said Government department who is provide 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 the written complaint form an affected person and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule(2).

v. Further the Government department shall preserve such information and associated records for at least ninety days for investigation purposes.

vi. In case, if the Government department does not comply with any of the above requirements of law, then the said Government department as also the concerned head of the department who is responsible for the social media facilities and the concerned IT head would be liable for civil and criminal consequences.

vii. The civil consequences could consist of being sued for damages by way of compensation upto 5 crore Rupees under summary proceedings before the adjudicatory authorities specially constituted under the Information Technology Act, 2000. Further if person wants, they can sue the said Government department for damages beyond 5 crore Rupees in a court of competent jurisdiction.

viii. In case the concerned Government department does not comply with all the aforesaid laws, the said Government department as also the person heading the department and the concerned IT head would also be liable for criminal liability which could range from imprisonment of 3 years to life imprisonment and fine which could range from 1 lakh to 10 lakh Rupees.

Rules for Privacy and data collection: While social networking enables greater transparency, it is equally important to ensure the protection of people from exposure to

inappropriate or offensive material.

- Since profiles on social network are linked more often to individuals and not organisations, for the organisation's site/page, a separate work profile may be created which can then be linked to a general email address that is accessible to anyone in the team, enabling them to administer the social networks without compromising on individual privacy.
- It is critical that social media policy for the Government is compliant with existing law governing data protection and privacy. Each department of the Government may be recommended to publish their own set of additional protections to safeguard privacy of citizens while maintaining highest levels of transparency of Government bodies.
- If the departments/agencies are collecting personal information on a social media platform, the same must be stated upfront. For example, while seeking inputs on a particular policy, it is may not be necessary to save the email id of each and every respondent and just saving the responses may suffice.

Identity Management: Identity management for the purposes of this document refers to management of identities of individual/s who seek to engage with government agencies on social media platforms. Such management relates specifically to registration mechanisms, delineation of personal identity from official identity of government officials and need to engage in a non-anonymous manner in such consultations. Towards this end, the departments may like to use following or any other suitable mechanism to achieve the above:

- Provide for activation of registration for engagement by seeking confirmation of email addresses
- Send acknowledgement/responses to queries to registered email addresses
- Providing official email ids and accounts to each and every government official authorised to engage on behalf of the department and permit use of only official accounts for engagement

However, while applying the above, The Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011 stated in the preceding paragraphs above must be complied with.

The relevant sections of the Information Technology Act 2000 are placed in Annexure III for ready reference. In addition, the users may refer to any other relevant legislations, provisions and

rulesnotified.

5.1.4 Communication Strategy

Some of key aspects of communication strategy include – Integration of Social Media into routine, Connection with existing networks, Sharing content across sites and Publicising use of social networking through traditional media.

- Social media can only be used by the Government to communicate existing Government information and propagate official policy to the public.
- While the social media tools allow everyone to become a creator, for the official account, content will have to be specified and tailored to the site on which it is being published.
- 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.

5.1.5 Creating Pilot

Since social media are relatively new forms of communication, it is always better to test efficiency and efficacy of such an initiative with a pilot project. Some of principles of creating such a pilot are given below:

- Focussed Objective setting: Initiate interaction for a limited objective or limited to one topic
- Begin Small: It is always better to start small and it is advisable to begin with one or two platforms.
- Multiplicity of access: The chosen platform should typically permit inputs from or linkages through multiple access devices. This will ensure wider participation.

- Content Management: It is not enough just register presence on a variety of platforms. It is essential that content provided is topical and up to date.
- Community Creation: On any social media platform, creation of a community is essential to generate buzz and sustain interaction.

A detailed guideline on creation and sustenance of community building is placed at

5.1.6 Engagement Analysis

Social media monitoring must be an integral part of any social media strategy. Social media data is different from other data or information because organisations have no control over its creation or dissemination on the Web and in order to understand and analyse the data a structure has to be imposed externally on it. Today a multitude of tools offer solutions for measuring conversation, sentiment, influences and other social media attributes. They help in discovering conversations about project and organisations and can be used to proactively engage with stakeholders. The Social Network Analysis (SNA) Software facilitates both quantitative as well as qualitative analysis by mining the raw data and combining it with individual and socio matrix. While some SNA software also have the features that enable them to import and/or store databases from social network, others perform preferential analysis to predict individual level or network outcome. Many social media monitoring platforms offer demographic information such as age and location. This information can be used to expand the reach of your platform by creating a geo-targeted campaign focused on areas that generate the most traffic to your social media site.

Some considerations for Data Analysis include:

- Data Definition: Selection of platforms, pages and/or organizations
- Depth and detail of analysis on each page: Areas or sections of the page to analyze (Wall, Discussion board, Pictures, etc.)
- Time-frame: Last one month etc.
- Criteria for determining the importance of the pages: notability, popularity, intentions/goals of pages, etc.

Some of challenges encountered in analysis may be related to

- Overlapping functions of posts: many comments and responses serve multiple purposes
- Difficulties in disentangling "push" messages from "pull" messages
- Inexhaustible range of topics that extend beyond your area of interest
- Unpredictable patterns of conversation and user exchange

These challenges may be mitigated by taking the following steps:

- **Limit Scope of Analysis**: Making a small start and defining Top 5 or 10 metrics may help organize the Data e.g. No. of mentions, No. of comments on specific posts, No. of retweets, No. of likes or shares etc.
- **Creation of Dashboard**: There are many free tools available that can help create a dashboard view of the data which can be pulled in through RSS feeds. This will help keep tab on latest happenings
- **Connect with responders**: It is a good idea to collate information/link to profiles about people who respond to queries or topics of your organisations interest, also observe their preference of response – individual mail, wall posting etc. Over a period of time this will help generate a broad profile of people who respond to your efforts
- **Follow the followers/Leaders**: Follow your followers and leaders on other networks/platforms to hear what is being talked about. This would help in spotting the trends in discussion.

5.1.7 Institutionalise Social Media

The final step in ensuring that the pilot is scaled and integrated is to link it to existing administrative and communication structure. An indicative list includes:

- Rules may be established that all policy announcements will be undertaken simultaneously on traditional as well as social media;
- All important occasions as far as possible may be broadcasted using social media;
- All documents seeking public opinion must be posted on social media sites;
- All updates from the website would automatically be updated on social media sites and;
- All traditional communications will publicize the social media presence.

VI. Conclusion

The Framework and Guidelines in this document have been formulated with a view to help government ministries, departments and agencies to make use of social media platforms to engage more meaningfully with their various stakeholders.

Social media's characteristics of connectedness, collaboration and community have the potential of ensuring broad based consultation, and can help agencies reduce the duration of consultation process and receive immediate feedback on services delivered.

In order to effectively utilize this media, the agencies must define very clearly the objective of such an engagement, select platforms that will be used for engagement, rules of engagement, communication strategy for ensuring broad basing such an engagement, and finally if found effective and efficient institutionalize such social media with mainstream engagement process.

Both in India as well as across the world, various government departments and agencies at federal, state and local government level are using this media. However, this is a dynamic and evolving area and continuous engagement and nimbleness of response to such an evolving scenario will determine the success of such efforts.

Annexure-I

Social Media Types

Kaplan and Heinlein in 2010 classified social media into six different types: collaborative projects, blogs and microblogs, content communities, social networking sites, virtual game worlds, and virtual social worlds. A brief description of various types of platforms is given below to help the agencies understand their main characteristics and also lists some of the currently popular sites in each of the categories as well as examples of use of such platform by Indian or other governments across the world.

- **Social Networking:** Currently, social networking sites are the most prominent platform of social media. It 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 the facilities such as chat, instant messaging, photo sharing, updates, etc. FaceBook with over 800 million users is one of the most well-known social networking site. A few Indian government departments and agencies are using FaceBook including, Prime Minister's Office, Planning Commission, Ministry of External Affairs and a few Municipal Corporations and Police Departments,etc.
- **Blogs**: Blogs are descriptive content created and maintained by individual users and may contain text, photos and links to other web sites. The main interactive feature of Blogs is the ability of readers to leave comments and the comment trail can be followed. A community of Blogs is referred to as Blogosphere and can be used very effectively to gauge public opinion. While many websites offer free space for blogging, this activity can also be undertaken on the existing government websites. Many government officials blog in their personal capacity on various issues. The Digital Engagement Blog of the UK government is an initiative to use the Blog format to for consultation on as well for pronouncement related to existing and proposed policies.
- **MicroBlogs:** MicroBlogs are similar to Blogs with a typical restriction of 140 characters or less, which allows users to write and share content. It can be done in the form of text message, instant message or even email. Twitter is a microblogging site that enables its users to send and read text based messages or "tweets" of upto 140 character length. These Tweets are posted on the user's account and the site allows others to "Follow" the user. While Tweets are public by default, they can also be restricted to just the followers.

Tweets can be generated via web, smartphone or even through SMS on some mobile phones. Due to limitation of characters, url shortening and content hosting services are often used accommodate posts that are normally longer. Twitter collects personally identifiable information of users and shares it with third party users. Twitter is estimated to have over 200 million users. Twitter is useful for short and crisp messaging and being used by Ministry of External Affairs, Chief Ministers of many states, Members of Parliament and Prime Minister's Office.

- **Vlogs and Video Sharing sites:** VideoBlogs or Vlogs are blogging sites that mainly use video as the main form of content supported by text. Such sites especially enable those who may have limited knowledge of English to also share their experiences over internet. Vlogs are an important category of content over YouTube – the largest video sharing site. YouTube is a video Live Casting and video sharing site where users can view, upload and share videos and even leave comments about videos. However, for upload and sharing registration is required. YouTube is a subsidiary of Google Inc. Since a picture/or in this case a video speaks a thousand words, it is an excellent platform for sharing progress about projects. Many government departments including DeitY and Prime Minister's Office have uploaded their promotional video content on YouTube.
- **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 a "Wiki" These multiple pages are linked through hyperlinks and allow users to interact in a complex and non-linear manner. Many wiki communities are "private" and are used for deliberating upon internal policies and for knowledge sharing. Currently, based on the information available, no official wiki on any Indian government policy exists. Wikis are a good option for undertaking "close" web based interactions. Normally the content on wikis are created as part of "Creative Commons" and are more inclined towards copy left rather than copyright. Some of the other popular social media sites include
- SlideShare – Similar to YouTube, here only presentations in PDF, PPT, KeyNote or Open Office format can be uploaded
- Orkut and LinkedIn – These are two other popular social networking site. While the former is an open site, the latter is primarily a business networking site
- Picasa and Flickr – These are photo sharing sites

Annexure II

Relevant section of Information Technology Act 2000

The Government departments need to realize that the moment they provide social media platforms/websites/portals/facilities on their existing websites, portals and platforms, they become a network service provider as they provide the services of providing such social media facilities on the network. As such, the relevant Government department becomes network service provider and hence intermediary under the Information Technology Act, 2000. Further when the said Government department provides such social media facilities on its network, it receives, stores or transmits any particular electronic record on behalf of another person or provides any service with respect to that record. As such they become intermediary under Section 2 (1) (w) of the amended Information Technology Act, 2000.

The moment the Government department becomes an intermediary, it is governed by its liability under Section 79 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.

The said conditions which need to mandatorily complied with the Government department to claim exemption for any third party data information or communication link made available or hosted by them in connection with social media facilities made available by the said department on their network are as follows:

1) The function of the Government department is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted
2) The Government department does not-
   (i) initiate the transmission,
   (ii) select the receiver of the transmission, and
   (iii) select or modify the information contained in the transmission

3) The Government department observes due diligence while discharging its duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
4) That the Government department as intermediary must not conspire or abet or aide or induce, whether by threats or promise or otherwise in the commission of the unlawful act.
5) That the Government department must immediately after receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the Government department is being used to commit the unlawful act, must expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.
6) The Government department must also comply with all applicable rules, regulations and notifications in regard to their activity of providing social media facilities on its network.
7) That the Government department complies with the Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011.
8) That the Government department also complies with the Information Technology (Intermediary guidelines) Rules, 2011.
9) That the Government department also implement reasonable security practices and procedures as envisaged under Section 43A of the amended Information Technology Act, 2000.

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

ix. The Information Technology (reasonable security practices and procedures & sensitive personal data or information) Rules, 2011 – These rules define for the first time in independent India what constitutes sensitive personal data. Sensitive personal data or information of a person means such personal information which consists of information relating to;—

(i) Password;

(ii) Financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) Physical, physiological and mental health condition;

(iv) Sexual orientation;

(v) Medical records and history;

(vi) Biometric information;

(vii) Any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

x. For the purposes of protecting such sensitive personal data, the Government has mandated that any legal entity who is processing, dealing or handling sensitive personal data must implement reasonable security practices and procedures.

xi. 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 provides social media facilities on which network sensitive personal data is going to be stored, processed or handled or dealt, the said Government department could be in breach of the law and could face legal consequences.

xii. Further under the Information Technology (Intermediary guidelines) Rules, 2011, since the said Government department who is provide 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 the written complaint form an affected person and where applicable, work with user or owner of such information to disable such information that is in contravention of sub-rule (2).

xiii. Further the Government department shall preserve such information and associated records for at least ninety days for investigation purposes.

xiv. In case, if the Government department does not comply with any of the above requirements of law, then the said Government department as also the concerned head of the department who is responsible for the social media facilities and the concerned IT head would be liable for civil and criminal consequences.

xv. The civil consequences could consist of being sued for damages by way of compensation upto 5 crore Rupees under summary proceedings before the adjudicatory authorities specially constituted under the Information Technology Act, 2000. Further if person wants, they can sue the said Government department for damages beyond 5 crore Rupees in a court of competent jurisdiction.

xvi. In case the concerned Government department does not comply with all the aforesaid laws, the said Government department as also the person heading the department and the concerned IT head would also be liable for criminal liability which could range from imprisonment of 3 years to life imprisonment and fine which could range from 1 lakh to 10 lakh Rupees.

The aforesaid is the current legal position in India which impacts Government departments providing social media facilities on their network. In the light of the stringent provisions of the law and the subsequent legal consequences for non-compliance of the law, it is therefore absolutely essential that the relevant Government department providing social media facilities must completely comply with all the above mentioned legal parameters as mandatorily stipulated by the Information Technology Act, 2000 as amended by the Information Technology (Amendment) Act, 2008 and various rules, regulations and notifications issued there under.

The specific legal provisions referred to above as extracted below:-

- **Section 2(1)(w) of the amended Information Technology Act, 2000** states as follows:
- "Intermediary with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places and cyber cafes."

- **Section 79 of the amended Information Technology Act, 2000**: Once the Government becomes an "[intermediary", its liability for third party data or information is specifically stipulated under Section 79 of the amended Information Technology Act, 2000. Section 79 of the amended Information Technology Act, 2000 states as follows:-

"Section -79 Exemption from liability of intermediary in certain cases

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if-

(a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or hosted

(b) The intermediary does not-

(i) Initiate the transmission,

(ii) Select the receiver of the transmission, and

(iii) Select or modify the information contained in the transmission

(c) The intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if-

(a) The intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act.

(b) Upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner."

Explanation- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

Section 43 A of the Information Technology Act, 2000 also has a bearing upon the subject at hand. The said provision states as follows:-

"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.—For the purposes of this section,—

(i) "Body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(ii) "Reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;"

Further the Information Technology (reasonable practices and procedures and sensitive personal data and information) Rules, 2011 define what is sensitive personal data in the following manner:-

"3. Sensitive personal data or information.— *Sensitive personal data or information of a person means such personal information which consists of information relating to;—*

(i) Password;

(ii) Financial information such as Bank account or credit card or debit card or other payment instrument details;

(iii) Physical, physiological and mental health condition;

(iv) Sexual orientation;

(v) Medical records and history;

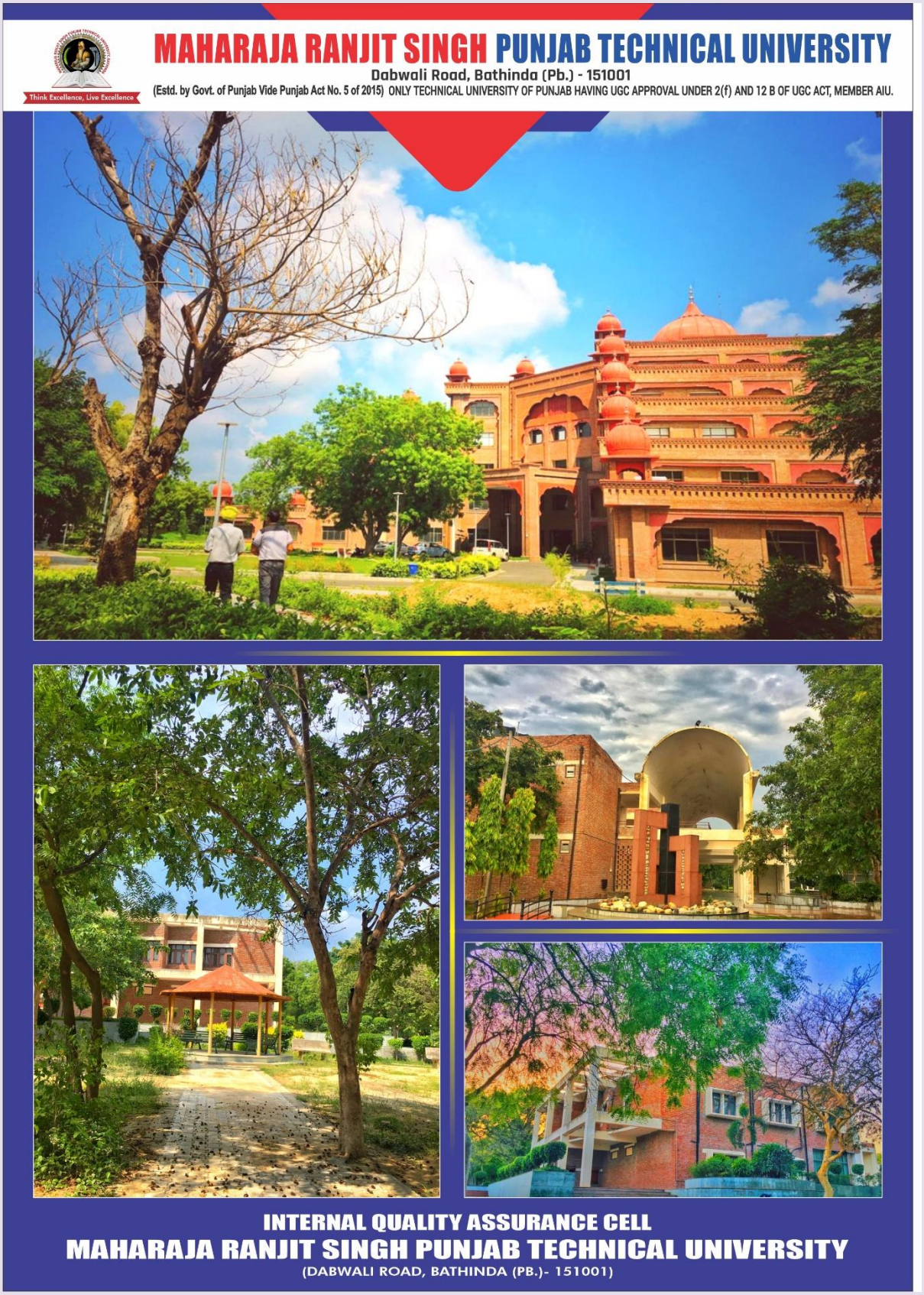
(vi) Biometric information;

(vii) Any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."

- The exposure for damages by way of compensation is upto Rupees Five Crores under the IT Act, 2000 and further criminal exposure ranges from imprisonment of 3 years to life imprisonment.


MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
Dabwali Road, Bathinda (Pb.) - 151001
(Estd. by Govt. of Punjab Vide Punjab Act No. 5 of 2015) ONLY TECHNICAL UNIVERSITY OF PUNJAB HAVING UGC APPROVAL UNDER 2(f) AND 12 B OF UGC ACT, MEMBER AIU.
Think Excellence, Live Excellence
INTERNAL QUALITY ASSURANCE CELL
MAHARAJA RANJIT SINGH PUNJAB TECHNICAL UNIVERSITY
(DABWALI ROAD, BATHINDA (PB.)- 151001)