الهيئة الاتحادية للموارد البشرية الحكومية
Federal Authority For Government Human Resources

United Arab Emirates

Digital Participation Policy In the Federal Authority for Government Human Resources

Last Update: May 2021

www.fahr.gov.ae

الهيئة الاتحادية للموارد البشرية الحكومية
Federal Authority For Government Human Resources

United Arab Emirates

Digital Participation Policy In the Federal Authority for Government Human Resources

ص.ب 2350، أبو ظبي، الإمـــارات العربيـــة المتحـــدة
هاتف T +971 2 4036000
PO Box 2350 Abu Dhabi, United Arab Emirates
فاكس F +971 2 6266767

ص.ب 5002، دبـــــي، الإمـــارات العربيـــة المتحـــدة
هاتف T +971 4 2319000
PO Box 5002 Dubai, United Arab Emirates
فاكس F +971 4 2959888

Purpose of the Policy:

This Policy provides a guide for employees of the Federal Authority for Government Human Resources on how to exploit Social Media Tools optimally, safely and effectively, for the purpose of communicating, and cooperating with the targeted audience in general.

Scope of the Policy:

The scope of this policy can be defined as follows:

This policy includes Social Media tools as defined in the glossary of terms contained in this document, which includes, for example, social networking sites, such as Twitter and Instagram. Social Media tools, blogs, etc. knowing that some of these tools may be owned by the Authority, such as the blog, while commercial sites, such as Twitter, are the other part of it.

This guide is not a reference to a specific tool or a website, but rather a guide that provides general guidance and instructions on Social Media tools. For instructions on how to use specific sites, such as Twitter and Instagram, you may refer to the Authority's Social Media department for more information.

This policy will constantly be updated to keep pace with the dynamic nature of s Social Media tools.

Introduction:

Social Media tools with their capabilities of cooperation and participation have surmounted the static web that depends on publishing and browsing, to become a new force that may shape the future of governments by reformulating their structures and public services.

More specifically, Social Media tools may help policy makers to set priorities, encourage the public to accept programs, increase levels of satisfaction and happiness, and thus enhance opportunities for success of policy outcomes. For example, Social Media sites - such as Facebook, YouTube, Twitter, blogging applications and mobile technologies - allow governments to engage in collective knowledge of society promptly and directly, thus, the targeted audience will transform from just passive users of government services

to consultants and innovators who contribute their ideas to meet their individual and group needs to a greater level.[1]

And the popularity of social networking sites is increasing around the world day after day, and despite this great popularity of social networking sites and the benefits that we mentioned above, However, the fundamental changes imposed by the use of these tools on the government and its relationship with the public have led to the emergence of many challenges and dangers that must be studied and dealt with carefully.

There are many ways to classify the use of social media tools in government, and here is one of the classifications of these methods:

Inside Participation- Involves sharing and exchanging internal policies and regulatory documents in government entities among them.

Outside Participation – Involves sharing information and common documents with various entities, bodies and individuals via government sites and applications.

Internal Participation - Like conducting an online poll on a government website.

External Participation – Sharing information with the public to engage them deeply in discussions via existing commercial sites, this type is the main focus of this policy.

Risks:

We must take necessary precautions to assess the risks associated with the use of social media, the most important of which are:

- The negative impact on employees productivity.
- Narrowing the broadband of the information network
- Possible damage to the reputation of individuals or the government entities
- The possibility of leaking government, personal, or any specific information of sensitive nature Security risks- such as phishing scams, social engineering, and the possibility of catching malicious programs, viruses, and other means of hacking

[1] United Nations 2010, United Nations e-government survey, New York, USA

Risks Reduction:

These risks related to the usage of social media networks can be mitigated by following a number of policies and procedures, including:

Applicable Policies and procedures:

These procedures define features of the conduct and content when using social network tools, such as those described in the various sections of this policy.

Acquisition Controls: It relates to logging in and subscribing to commercial social media sites which allow a high level of protection and privacy settings and more control over information (like setting strict verification measures or cookies). Examples of these controls can be found in the "Accessing Social Media" section of this policy.

Training Procedures: educating staff on the mechanisms of social networks and raising awareness among them of these tools by introducing them to the contents of this policy, behavior and best practices regarding the use of social media tools.

Requirements for Applying the Social Media Tools Usage Guide:

Most government entities in the United Arab Emirates are accustomed to dealing with indicative guidelines and regulatory policies such as those related to information technology, however, social media tools policies may be a different matter, therefore the successful implementation of the indicative guidelines provided in this policy requires the Authority's willingness to make the following arrangements:

The government entity is expected to assign a specific unit (administration or department) within the Authority with the responsibility of explaining this guide and familiarizing employees with it, monitor the extent of compliance with its directives and deal with all issues related to social media tools. Each entity may choose a department or administration that best suits this role, which may be - without limitation – the media, public relations, human resources, information technology or knowledge management or a joint committee that includes representatives from various relevant departments in the entity. In all cases, it is not recommended to appoint external suppliers for this mission.

Whereas most of the activities on the social media sites include the participation of the public in making decisions of some government policies or services, therefore, the selected department should develop a clear communication method with other departments of the entity to be responsible for designing or providing these policies / services. In addition, this unit should define the indicators necessary to measure the performance of government employees, and the impact of interaction with the public through social media tools.

Parallel to the implementation of this guideline - the Authority should maintain ongoing training and awareness-raising programs, with the aim of enhancing staff understanding of the benefits and dangers of social communication of social networking tools.

Additionally, government entities are encouraged to review and update their strategies and decision-making mechanisms, besides designing and delivering service. This is in order to ensure the promotion of e-participation across social media and measure the tool's adoption impact.

Indicative Guidelines Using Social Media Tools:

Below is a detailed explanation of the guidelines for using social media and this includes eight areas: access to social media tools, accounts management, employees conduct, content management, privacy security, other legal issues and audience code of conduct.

Access to Social Media Tools:

Employees can use social networking sites during working hours or through utilizing government resources (such as computers), some entities rather grant a specific number of employees access to social media tools as well as specifying a list of sites they are allowed to access.

The following requirements must be practiced at all times:

The main motivation behind granting employees the right to access social media networks is to improve their work performance and contribute to developing work outcomes and planned outputs.

In general, employees use Social Media sites during working hours for the following reasons:

- To manage the federal entity account
- To obtain information and services related to the nature of their work through their personal accounts on these sites
- To use it for personal or non-work related reasons.

It should be noted that it is difficult to draw boundaries between the employee's use of social media sites for professional or personal purposes, which makes the issue of granting the right to access for one reason rather than the other difficult.

Originally, access to all social media sites must be available to employees, provided that the employee shall be responsible for using these sites in accordance with this guideline and with the applicable employee code of conduct; accordingly, the employee will be responsible for any wrong or inappropriate use of those sites.

Blocking the access of some employees to social media may not be effective at all times due to the ability of many of them to access these sites through other channels such as mobile phones.

Due of the evolving nature of social media tools, it is preferable for the unit responsible for social media tools at the government entity to develop a list of preferred sites to benefit from. Take into consideration the necessity of developing this document in cooperation with the relevant departments such as information technology and with the employees themselves instead of being issued directly from the higher management of the entity. And take into account that this document is developed in cooperation with the relevant departments such as information technology and with the employees themselves instead of being issued directly from the higher management of the entity.

Account Management:

The process of managing an account on social media includes many areas, often referred to as "Life Cycle Management", and among these areas:

- Account creation
- Account Management
- Delete or disable the account

Creating an account provides the user with access to a variety of communication and collaboration tools, such as sending comments, chatting, blogging, and communicating with other users, which varies from one site to another. As we mentioned in the previous section, there are two types of accounts that employees may have on social media, below are the details for managing these accounts:

Managing the official accounts of the Federal Authority for Government Human Resources on social media:

In this case, the employee is authorized to communicate officially with the public via social media on behalf of the government entity, and all comments and opinions expressed by this employee represent the official view of that government entity. In this case, the following requirements must be achieved:

- The approval of the unit concerned with social media on the decision to create an account on social media sites as an official account of the Federal Authority. However, before making this decision, the unit must consult the IT unit to obtain an advice about the risks or requirements related to the technology such as security or privacy setting, in addition to that, all other relevant units should be consulted. This approval should take into consideration several factors such as the suitability of the site to the needs of the Authority and the public.
- The decision to establish the account should be documented according to the internal regulations of the government entity, and should specify that - in addition to the name of the social communication network – the name and position of the employee (or employees) who will be responsible for managing this account. It also preferable that the decision defines the topics or services that the employee can discuss with the public through this account

Take the following factors in consideration when assigning the responsibility of managing the account to any of your employees:

- Awareness of topics that he\she will discuss with the public.
- The language skills he/she has.
- They should be familiar with social networking sites.
- The willingness of the employee to communicate with the public through social networks outside official working hours, and throughout the week, and his/her ability to handle situations that may require an immediate response in these times.

- Employees - once they have been given authorization to use their names to represent the government entity on social networks and communicate on its behalf - should fully identify themselves, their designation, and contact information.

Managing Personal Accounts for Work-Related Purposes:

Employees may access social media networks through their personal accounts to obtain information or news necessary to carry out their job responsibilities (or for personal purposes as mentioned in section 1-5). In this case, employees may benefit from the resources and information social networks offer in order to complete their daily responsibilities. Since employees are responsible for managing their personal accounts on these sites, they are expected to act in accordance with the guidelines set out in Section 3-5 (Employees Code of Conduct).

Employees Code of Conduct:

In all cases, the behavior of the government employee should not be any different when using social networking than when using any media or communication tool which is subject primarily to the document "Principles of professional conduct and ethics in public office of the federal authorities," and the UAE Human Resources Law and its regulation in the UAE, and this does not only address the employee's conduct on social media, but also addresses the acceptable use of government resources and information, and this includes for example:

- Employees should demonstrate best ethical principles.
- Use public funds with honesty and transparency, and avoid wasting funds.
- Employee should refrain from using the information obtained during the performance of his/her duties for other purposes than work.

In addition to these requirements, and in order to ensure that government employees distinguish between their professional positions and their personal activities and opinions, employees must adhere to the following guidelines when using social media networks in their personal capacity, whether to meet work-related or personal needs:

- He/she should not publish official communication information in personal accounts on social networking sites for purposes of communication. This information includes e-mails, phone numbers and P.O Boxes.

- An employee may mention his/her occupation in the personal identification files on his personal account on social networking sites. But in this case he/she has to clearly state in the disclaimer that what is written in the comments on this site represents his/her personal opinion and is not linked to the government entity.
- In all cases, the employee is responsible to ensure that his personal behavior does not affect the governmental entity's social networking sites negatively.

Content Management:

The Authority is responsible for publishing and managing the contents of its pages on government and commercial social networking sites. This responsibility should be assigned to the organizational unit responsible for publishing and managing the Authority's content through traditional media. However, the following characteristics of social media should be taken into consideration:

- Communication with the public through social media tools is interactive, not authoritarian, as it is targeted communication and is not random or general as is the case when communicating using traditional means of publication; this allows the Authority to broadcast the right message to the concerned public quickly and directly.[2]
- Promoting a collaborative environment is the key to creating successful digital communities, engaging in meaningful dialogue and contributing to a constructive link between the Authority and the public.
- The content submitted by users represents the majority of the content posted on social media, which may raise legitimate concerns about the reliability of this content, in addition to the challenge of coordinating user content or controlling participant behavior.

- The style of discussions via social media tools is often spontaneous, informal and unexpected.

[2] Hrdinová, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany: Center for Technology in Government

- Participants in the Authority's page on social media can refresh the page at any time, even outside of working hours.

In light of the above, the Authority should take appropriate decisions regarding the following matters:

- Selection of employees who will conduct the content management of the Authority's account and interact with the public, the previous characteristics of the social media tools in addition to the advice provided in Section 6.3 (Account Management) can help in making this decision.
- "Life Cycle Management" the content posted on social media, hence managing to delete / remove information that may become irrelevant for one reason or another (such as the information of the customer service employee when he/she quits to work for the Authority)
- Adoption of the coordination strategy - if any- to manage user-submitted content. Coordination is considered important to ensure appropriate behavior, which should be practiced carefully so as not to restrict the aforementioned cooperation and participation. Participants should be clearly educated, to define their expectations and direct their contributions. Therefore, the user's contribution must be preserved as long as it is within the context of the post - regardless of whether it is negative or positive - otherwise, the content may be deleted if it constitutes a type of infringement or offense.

There are several coordination strategies that you can choose from:

- User-end format: Where the user may choose to perform the self-blocking according to the code of conduct, which must be published explicitly on the website, and this coordination is the least restrictive form of coordination, It also requires the least amount of resources, however it represents the greatest risk of posting inappropriate content.
- Formatting by the user community: An example of this is the reporting of infringements. This type of coordination allows the manager to evaluate reports from users about inappropriate content, and to take appropriate action.
- Formatting by the manager: The manager monitors all types of content while it is being sent, and has the right to delete the content whenever it violates specific criteria (see section 7-5 : Public Code of conduct)

- Pre-formatting of the content: (It is intended to filter all content sent before it is allowed to appear), which allows for greater supervision, however it reduces the speed of exchange / dialogue between people, It also requires a reasonable amount of resources.
- Formatting the content after posting: here, the Authority allows users to send commentaries on their pages on the social media site, which will be displayed immediately, and intervention is not made until later when reporting cases of infringement
- Automated Format: Where a filtering program is set up, it automatically places references to combinations of keywords that managers have classified as spam, and then the content is manually reviewed to assess its suitability.

Security:

The risks related to security is among the most important and main risks and challenges concerning the use of social media, these sites which include for example blogs, social networks and Wiki tools are more prone to three different types of security risks, which include: Phishing, Social engineering and cyber-attacks (see appendix A- Glossary)

In general and when appropriate, the Authority's security policies shall apply to social media tools, however these entities must also take the following measures:

- Ensure that employees do not use their official government email address or password to log in to their accounts on social media.
- Blocking access to unneeded applications (such as electronic games) in some social media sites in some social networking sites, in order to avoid potential security and hacking risks.
- - Educating staff on the potential threats of using social media, especially risks related to social engineering and the prevention methods.

Privacy:

As with security risks, subscribing to social media sites increases the chances of privacy breaches which is the inappropriate use of government information by people who are not authorized to access such information. Although no privacy law has been adopted in the country, the Authority should take all necessary measures to ensure that the privacy of government data and information is protected from any potential privacy risks that may arise from social networking sites, therefore, the following requirements should be implemented:

- The Authority should clearly specify the type of information that employees may post on social media sites.
- Employees should be aware that there is no privacy on social media sites, comments sent to those sites remain there for a long time, and visitors to those sites may view these commentaries and copy them to other sites, without requiring permission from the sender.
- Employees should be careful when sending or submitting information to social media, so that they can protect sensitive government information, such as confidential data or customer information in addition to their personal information.

Audience Code of Conduct:

The main objective of using social media is to maximize the level of communication between the Authority and the public, effectively and with minimal risks, hence, a code of conduct for the public should be prepared to clarify the proper behavior of users, and it should be placed in a clearly in the site in order to facilitate quick reference.

- Irrelevant or out of context.
- Comments that undermine or abuse beliefs
- Comments that promote discrimination
- Comments that may contains a breach of intellectual property rights

Other Legal Matters:

The use of social media sites raises justified concerns related to legal concepts of copyright and intellectual property. The ease of publishing content and its distribution in social networking sites makes it very easy to breach copyright laws unintentionally.

It is necessary that all governmental entities publish a clear disclaimer on their social media pages to retain copyrights and publishing rights. It should also refer to the Law of copyright of the United Arab Emirates No.7 in 2002. Finally, government entities must always be aware of the difficulty to protect the copyrights of printing and publishing content onto social networking sites. Therefore the content should be carefully chosen and revised before publishing.

And even in case of establishing copyrights, another issue that should be taken into consideration is the issue of storing and keeping information on social networking sites, and whether or not this information will be a public record, and then allowing everyone to review such that information and access it.

It is noteworthy to mention that most government information is a public record, and information sent to government websites or by government officials to social networking sites can be classified as public, Clarifying and identifying distinctions will help in dealing with information, storing and disposing of it in the long term.

Appendix A- Glossary

• Social media tools: These are tools allocated for social interaction and communication by sing publishing techniques that make it easier to access and increase capacity automatically. Social media uses these means to enable individuals to produce content and share it with others. These sites also support the democratization of knowledge and information, and convert people from mere consumers of content to partners and producers.[3]

- **Social media section**: We use this term in this document to refer to the organizational unit responsible for managing the Authority's presence on social media, and take all decisions related to social media, and it is recommended that this unit be the media or public relations unit
- **Social media owned by the government**: These are the social networking tools or sites owned by the Authority such as blogs on any site of government websites.
- **Commercial social media**: Social networking sites that are not owned by a government entity. Examples include social networking sites (like Facebook & Twitter), or blogging sites (such as Word Press).

[3] http://en.wikipedia.org/wiki/Social_media

- **Phishing**: is a cyber-attack which targets a user or a certain group of users contacted by luring individuals into taking a specific step, such as opening a document or clicking a link, which leads to the start of the attack
- **Social Engineering**: Social engineering is a malicious activity and is considered as a threat to security, it is a psychological manipulation of people into performing actions or divulging confidential information, such information could be collected from the user's account from social media.
- **Web Applications Attacks:** Web applications means dynamic web pages that use text to provide additional functionality to a user, social networking is considered an advanced web application, and its use requires an advanced level of interaction and capabilities, which makes these sites vulnerable to a wide range attacks.

Social Media sites: Sites or applications that allow users to (1) compile an introductory file, (2) communicate with other users within the network (3) participate in dialogue, discussion and cooperative activities between participants (4) publish contents in order to
share it with other users browsing the site or application.[4]

Blogs: a **blog** (a truncation of "weblog") is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries (posts) contain all the information about a particular topic with the possibility of including multimedia images and video clips. Posts are typically displayed in reverse chronological order, so that the most recent post appears first, at the top of the web page.

[4] Al Shair, S., Elbadawi, I. (Forthcoming). Social Network Sites and e-Governance: Designing Effective Policies for Government Organizations