SOCIAL MEDIA POLICY

October 2023

Review Period

This policy is for the period from October 2023 to October 2024. The policy will be reviewed by the Director of Communications and updated as needed in October 2024.

Appendices will be updated at the discretion of the Director of Communications.

INTRODUCTION

Aims of This Policy

This policy is intended for use by the Cayman Islands Government (CIG) as a reference for acceptable and unacceptable use of social media accounts. It serves to:

- Offer advice and guidance on content staff can post on social media platforms
- Help Chief Officers to direct resources and training appropriately within their remit
- Comply with laws, policies and codes of conduct
- Improve the quality and effectiveness of social media interactions between the Cayman Islands Government and the people it serves

This policy may be used as reference for Statutory Authorities/Government Companies (SAGCs) in addition to government agencies. SAGCs may choose to adapt and create their own guidance based on this document.

Scope of This Policy

This policy offers staff using social media either for personal use or for sanctioned official use, as well as contractors managing official CIG accounts, a framework for posting on social media networks.

This policy extends to work and at-home use of social media by staff, following the Public Service Management Act (2018 Revision). It does not pertain to private or confidential communications online – such as email or conversations – but at the same time it is expected that public servants will observe the Public Servant's Code of Conduct, reproduced in **Appendix 1** of this document for reference, in all areas.

While this policy applies to personal and official use, the content guidelines refer to use of social media platforms as authorized public servants, representatives, ministries/portfolios, or departments.

Updates to This Policy & Review Period

This policy is for the period October 2023 to October 2024. The policy will be reviewed by the Director of Communications and updated as needed from October 2024.

Appendices will be updated at the discretion of the Director of Communications.

WHY USE SOCIAL MEDIA

About

1. Given that 4.88 billion persons globally use social media it is clear social media is a part of daily life. Specifically, within the Cayman Islands, 60.8K persons are active social media users. *(Digital Global Statshot Report, Datareportal.com, July 2023)*

2. In a 2022 survey, 88% of the Cayman Islands population reported using WhatsApp and 47% of reported the use Facebook regularly. CIG has a strong channel penetration on Facebook and LinkedIn. The channels with the greatest opportunity to grow CIG's presence and follower base is on WhatsApp, YouTube and Instagram. *(Channels Performance & Usage Report 2023, Department of Communications)*

3. It's clear that in the Cayman Islands, people use WhatsApp, Instagram, Facebook and other social media sites as a source of credible information. Internationally, this figure is also growing. It makes sense to use social media accounts to disseminate information and engage with the wider public.

Personal versus Official Duties

4. When using your own social media accounts, and where not commenting as an authorized public servant, or representative, we consider this to be personal use of social media.

5. For personal use of social media, when you are identified or identifiable as working for the CIG, you should follow the Public Service Management Act (2018 Revision), including the Public Servant's Code of Conduct (Appendix 1) and other relevant policies. **Our employees must not**:

    - Link your personal social media accounts to a government email address
    - Use accounts in such a way as to interfere with your duties (responsibilities and time) or breach the Public Servant's Code of Conduct
    - Post fraudulent, harassing, threatening or otherwise unprofessional or unlawful materials that would bring your employer or the CIG into disrepute
    - Post confidential or sensitive information obtained in the course of their work

6. When using social media accounts for official duties, including commenting as an authorized public servant, or representative, or as a ministry/portfolio or department, we request that you:
    - Are respectful and helpful
    - Use government email addresses linked to government accounts
    - Remain objective and unbiased
    - Do not post fraudulent, harassing, threatening or otherwise unprofessional or unlawful materials
    - When publishing content, remain impartial and apolitical, and represent the

government of the day.

- Otherwise follow the Public Service Management Act (2018 revision), including the Public Servant's Code of Conduct (**Appendix 1**), and other relevant policies.

Risk

7. While social media is an invaluable tool for communicating and engaging with the public, there are some risks associated with social media that you must consider before using it for Government purposes. These include:
    - Misinterpretation/messaging: There is always room for misinterpretation online because tone can often be lost without context. Be aware of this, and post clear messages online.
    - Lack of control: Once a post is public, the ramifications of the message are somewhat outside of your control. What you can control is how you approach reactions.
    - Resourcing: Social media can become somewhat draining on time and resources within a department if expectations are not managed correctly.
    - Privacy: It is possible for confidential and private conversations on social media to fall into the public eye and for personal data to reach a very wide audience and be further shared in ways which you are not able to control. With that in mind, we always recommend cautious use of private discussions with members of the public and of any personal data.

8. When it comes to reputational management, crisis communications, and risk assessment, the Department of Communications is available to support you. Contact the communications team at communications@gov.ky for more information.

Copyright

9. Intellectual property and copyright on social media are governed by The Copyright (Cayman Islands) Order 2015 and the Digital Millennium Copyright Act (DMCA).

10. Put simply, do not use materials, images, videos or content without the permission of the owner on social media. Where in any doubt, do not use content that you do not own on social media channels.

Endorsement

11. Following, liking, or sharing information on Government channels is not an endorsement of a link or account – but some care must be taken regardless. Do not share or like posts or links that are controversial, or otherwise pose an institutional risk, or are unprofessional. Do not share posts that are against our tone and values.

12. We only share trusted and verified sources of information. If you are unsure whether to share something, do not share the post. We do not share posts:
    - containing misinformation and unverified news
    - that use offensive or use of inappropriate language
    - that include memes, tabloid content or clickbait
    - that endorse alcohol, drinking, or drug use
    - including inappropriate (e.g. vulgar, offensive etc.) user names or language

- that promote discrimination based on race, sex, sexual orientation, religion, nationality, disability or age
- that infringe any copyright, database right or trade mark of any other person
- that are likely to harass, upset, embarrass, alarm or annoy any other person
- that give the impression that the contribution emanates from the Government if this is not the case

13. We do not provide opinions on commercial businesses or favour one business over another.

14. In personal biographies of accounts that explicitly post Government materials, remind your audience that you are not posting for or on behalf of the Government (for example, in a Twitter bio say “all tweets are my own”).

Processes for the Release of Content & News

15. Content and media related activities are confidential until released through official Government channels. News and media-related activities must be coordinated and approved by any involved Chief Officers. The Chief Information Officer has oversight of the release of news and will coordinate the release through official Government, and not personal, channels first.

16. While civil servants are encouraged to share Government content and news, civil servants should not present themselves as a primary news source without first using the appropriate Government channels.

Social Media Contractors & Agencies

17. Any vendors or contractors acquired to carry out social media tasks on behalf of the Cayman Islands Government must be acquired through due diligence and proper procurement. Contractors involved with Government social media have access to personal data and must maintain the reputation of the Cayman Islands Government.

18. All vendors and contractors are utilized at the risk of the content owner. The content owner should provide written approval to vendors or contractors.

19. The main Cayman Islands Government social media networks will not provide vendors or external contractors logins to these accounts, unless at the explicit direction of the Director of Communications.

Privacy & Information Security

20. When users contact authorized public servants, representatives, ministries/portfolios, or departments they expect their information to be treated confidentially.

21. If personal data has been collected in the course of delivering Government programmes and services, individuals will also have legitimate expectations about how their data may or may

not be used. This includes on social media for promotional and similar purposes, which are secondary to the original purpose of receiving a service or participating in a programme offered by the CIG. Other official information you have access to in the course of your duties should never be published on social media.

22. When using social media services, there are cyber risks around fake requests from spam profiles, phishing emails, brand impersonation and ransomware. On social media websites like Facebook and Twitter, there are users who create fake accounts to spread spam emails and malicious malware. Fake social media accounts are created for our public figures, organisations, etc., that look very similar to the actual profile of our public figures or organisations. These are used to attract unsuspecting customers towards them, for the purpose of stealing confidential information and fraudulent purposes. Today, businesses are also falling prey to brand impersonation as most of the hackers may promote false things on duplicate profiles of businesses and organisations. False activities conducted on such profiles will send the wrong message to our customers.

23. Don't click on suspicious messages or links, even if they appear to be posted by someone you know. Report any scam posts or messages you encounter on social media to help stop the threat from spreading.

24. Always report such posts or messages to the platform's abuse mailbox. If they pertain to our public figures, it is very important that you also report them to the Chief Information Security Officer for Government via the email address Cyber_Helpdesk@gov.ky

25. Use unique, complicated passwords for all your accounts. If the site offers multi-factor authentication, use it, and choose the highest privacy setting available.

26. Be aware of the risk of logging into your social accounts while using public Wi-Fi, since these networks are often unsecured and your information could be stolen.

27. If you are a civil servant, ensure you complete Cyber Awareness Training which is accessible via the Civil Service College.

28. As a general rule, do not disclose names, pictures, personal data, or other information on social media if it is unnecessary or if it relates to confidential or sensitive matters, business information that is considered privileged or commercially sensitive, or individual service users without prior consent or another lawful basis being identified as well as appropriate approval.

Defamation & Negligence

29. The way we treat our audiences is of the utmost priority.

30. In the Cayman Islands, defamation takes place when an individual publishes words or images that contain untrue assertions about a third party where it undermines reputation in some way. This carries a hefty sentence if found to be criminal.

31. With this law in mind, when using social media in any capacity, we advise our staff to not do anything that could be considered discriminatory, or make offensive or derogatory comments online.

32. As a general rule, if you are unsure whether your comment or post falls into a defamatory nature you should not be posting this online.

Record keeping

33. As a public agency, you are responsible for managing social media records. When using social media as an authorized public servant, or representative, or as a ministry/portfolio or department you are responsible for record keeping – you cannot rely solely upon the social networks in use. To this end, we recommend the use of scheduling platforms such as Hootsuite to perform the function of record keeping as you can download all posts from this platform into excel spreadsheets with ease.

34. At a bare minimum, controllers and managers of social media accounts for authorized public servants, representatives, ministries/portfolios, or departments, should download a record of their social media activity once quarterly since social media networks have no legal obligation to retain records. These downloads should then be managed alongside other records and information as part of your agency's file plan.

35. If you are unsure of how to download these records contact communications@gov.ky

Information Rights

36. Government is accountable to the people we serve. We should be transparent, engage the public, and respect and promote individual rights in our social media presence.

37. The Data Protection Act, 2017 governs the collection and use of personal data. On social media, you must be particularly attentive to the principles relating to fair and lawful use, data minimisation, data accuracy, and respect for individual rights. Individuals who are identified or identifiable in your posts should be aware their data may be used this way before publication. If an individual asks you to stop processing their personal data by removing a post about them or their photograph, you must comply with this request.

38. The Freedom of Information Act (2020 Revision) provides a general right of access to Government records, with limited exemptions which balance this right against other rights and the public interest in not disclosing information that would cause some harm. It also encourages agencies to proactively make information available – particularly where it relates to our public functions, how to access programmes and services, and how decisions are

recommendations are made. Requests for information may be submitted through social media and should be dealt with the same way as emails.

39. For issues relating to data privacy, access to information, notices to stop processing personal data and other matters, the Information Rights Unit is available to support you. Contact the team at informationrights@gov.ky for more information.

Escalation policy

40. Identify what urgent inquiries could look like for your account ahead of time, and be ready to escalate comments and interactions where needed.

41. You should also be aware of the rights which individuals have to complain, seek records or information, or request some action be taken in relation to their personal data. Where comments or interactions amount to an individual making a complaint that may escalate to an investigation by the Ombudsman under the Complaints (Maladministration) Act (2018 Revision) or Data Protection Act, 2017; requesting records under the Freedom of Information Act (2020 Revision); or seeking to exercise rights in relation to their personal data under the Data Protection Act, 2017, these matters should be immediately flagged to your Information Manager or Internal Complaints Process Officer.

42. High level issues should be made known to heads of departments before crafting a reply. A statement may need to be prepared and shared, in which case GIS can support and create this for you.

43. By making communications colleagues and heads of departments aware of high-level issues you can ensure that any responses made by your account are in-line with Government policy.

Creating a Social Media Account

44. Departments, Ministries/Portfolios should not create new social media accounts without prior consultation with the Department of Communications.

45. Authorized government channels are responsible for telling the truth, remaining unbiased and engaging with people online.

46. If you cannot engage with questions and comments online, you do not have the resources to use the channel and you should consider working with the CIG channel to communicate your content effectively.

Further Guidance & Advice

47. The primary contact for further advice relating to social media and the social media policy is the Public Engagement Officer in the Strategic Communications Unit. For more guidance on social media and any updates to the policy, contact communications@gov.ky

APPENDIX 1: PUBLIC SERVANT'S CODE OF CONDUCT

(a) A public servant must behave honestly and conscientiously, and fulfill his/her duties with professionalism, integrity and care;

(b) A public servant must be courteous and respectful to the Governor, the Speaker and Deputy Speaker, Official Members, Ministers, Members of the Legislative Assembly, other public servants and members of the public, and treat everyone with impartiality and without harassment of any kind;

(c) A public servant must be politically neutral in his work and serve the government of the day in a way that ensures that he maintains the confidence of the government, while also ensuring that he is able to establish the same professional and impartial relationship with future governments;

(d) A public servant, as a member of the public, has the right to be politically informed but must ensure that his participation in political matters or public debate or discussions, does not conflict with his/her obligation as a public servant to be politically neutral;

(e) A public servant must not at any time engage in any activity that brings his ministry, portfolio, statutory authority, government company, the public service or the government into disrepute;

(f) A public servant must obey the law and comply with all lawful and reasonable directions, including work place rules established by his/her Chief Officer or a person with delegated authority from the chief officer;

(g) A public servant must disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) with his/her duties as a public servant, and must not use his/her official position for personal or familial gain;

(h) A public servant must treat all official information and any dealings with the Governor, an Official Member or Minister as confidential, and, unless authorized to do so, must not give or disclose, directly or indirectly, any information about official business or anything of which he/she has official knowledge;

(i) A public servant must not use official resources, including electronic of technological resources, offensively or for other than very limited private purposes.