Crime and Corruption Commission
QUEENSLAND

Corruption Prevention Advisory July 2017

Social media and the public officer

In this advisory:

This advice highlights the risks and offences of social media use by public officers.

It covers:

- Appropriate use
- Risk factors
- Liability for misuse
- Best practice advice for public officers
- Strategies for agencies to prevent misuse
- Further information and resources on social media use.

Introduction

Social media allows us to engage and communicate with our customers and colleagues to build stronger and more successful relationships.

Social media consists of online interactive technologies through which individuals, communities and organisations can share, co-create, discuss, and modify user-generated content or pre-made content posted online. These technologies include:

- messaging technologies such as email, SMS, WhatsApp, QQ Chat (China), WeChat (China), LINE (Japan)
- social networking sites such as Facebook, Yammer, Weibo (China), Myspace, Google+ and LinkedIn
- mass communication platforms such as Twitter, Reddit, Viber, Qzone (China) and Tumblr; and
- video and image sharing platforms such as YouTube, Pinterest, Snapchat, Instagram and Flickr.

However, as social network platforms are open forums, public officers must understand the responsibilities and obligations that come with the use of social media for both official and personal use.

Official uses

- for public business use – most commonly a department's Facebook page or Twitter account
- for internal business use – for example, Yammer

Personal uses

- personal use from official facilities or devices
- private use from personal devices during work time or out of work time.

Appropriate use

While public officers have the right to contribute to public discussions on community and social issues in their private capacity, they must be aware of and adhere to their obligations as public sector employees.

Public service employees are bound by the *Code of Conduct for the Queensland public service*[1] (The Code) which states that employees will:

a. take reasonable steps to ensure that any comment they make will be understood as representing their personal views, not those of government
b. maintain the confidentiality of information they have access to due to their roles, that is not publicly available, and
c. be aware that personal comments about a public issue may compromise their capacity to perform the duties of their role in an independent, unbiased manner.

Public sector entities will have their own Codes of Conduct which reflect these principles.

Social network platforms are readily accessible public forums and anything posted on them has been published. The person posting or publishing material will have some control over the initial audience but no control over how their material is used by others once it is published.

There is also no real anonymity on social media. Following a series of landmark legal cases, Twitter, Google, Facebook, Microsoft, Yahoo and other providers have accepted that they can be compelled to reveal the identities of people who post under pseudonyms or avatars. Many of these providers no longer oppose applications to reveal the identity of users.

Risk factors

Inappropriate use of social media can result in:

Disinformation

- creating the wrong impression by using humour, irony or satire which can be misunderstood in impersonal or abbreviated formats
- misleading the audience by sending information that is inaccurate, incomplete, out of context or confusing.

Reputational damage

- damage to government reputation through private commentary on government policy - this commentary may be misunderstood as being a statement in an official capacity or as representing the views of government
- damage to work relationships through unprofessional use of internal social media.

Breaches of privacy

- sending a message to the wrong person
- unlawfully releasing confidential or personal information[2] obtained through your employment.

1 Code of Conduct for the Queensland public service 1.3 Contribute to public discussion in an appropriate manner.

2 Personal information is information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion – *Information Privacy Act 2009* s. 12.

Security risks

- identifying yourself as a public officer and thus inadvertently providing opportunity for your identity to be used by others to perpetrate fraud either on your organisation or in the name of your organisation and thereby damaging your organisation's reputation.

Liability for misuse

Code of Conduct – content published on your personal social media account that is:

- about your organisation, or
- information obtained in the course of your duties, and
- not in line with your organisation's values, Code of Conduct or policies,

may result in disciplinary action against you regardless of whether the information was published during or outside work time.

Agency ICT use policies – Limited personal access to and activity on personal social media sites using your organisation's equipment is generally permitted. However, use must be in line with your organisation's Communication policy and ICT security guidelines. Any failure to follow these guidelines may constitute a breach of the agency's Code of Conduct and lead to disciplinary action.

QGCIO guidelines and IS 18 Information security policy documentation – Under QGCIO's Information Standard 18, agencies must develop, document, implement, maintain and review appropriate security controls to protect the information they hold. Breaches of your agency's policies and procedures may constitute corrupt conduct[3] which could result in dismissal and/or civil legal action against the individual and organisation involved.

Consequences can also include being charged and convicted of various criminal offences under the *Queensland Criminal Code* including official corruption, computer hacking/misuse, misconduct in relation to public office, abuse of authority and other offences. These offences carry various penalties of imprisonment for up to 10 years.

Public Records Act 2002 – Yammer postings, messages, attachments and polls are digital public records under the *Public Records Act 2002*. Queensland State Archives provides information on Recordkeeping which covers what content needs to be captured and how to capture it.

Best practice advice for public officers

- Keep up-to-date with your agency's policies including the Code of Conduct, ICT policies, Recordkeeping policy and procedures, General Retention and Disposal Schedule and social media policy and procedures.
- Familiarise yourself with the Office of the Information Commissioner's information on applying privacy principles to social media:
  - using social media in the course of your employment – *Social media checklist*
  - using Yammer – *Yammer. A private social network?*
- When using work-related social media, communicate in a way that is transparent, accurate and adds value to your work relationships.

3 The *Crime and Corruption Act 2001* s. 15 defines corrupt conduct as conduct that involves the exercise of a person's official powers in a way that is not honest or not impartial, or involves a breach of the trust placed in a person as a public officer, or involves a misuse of official information or material, and would, if proven, be either a criminal offence or a disciplinary breach providing reasonable grounds for dismissal.

- Be responsible with your use of personal facilities or devices. What you post on social media from your own facilities or in your own time is not a private conversation. In both law and practice, anything posted on social media has been published for anyone to read (despite your privacy settings), and can be widely distributed without the consent or knowledge of the person who posted it. The *Public Service Act 2008* s. 187 specifies that any "*inappropriate or improper conduct in a private capacity that reflects seriously and adversely on the public service*" may result in disciplinary action being taken against you under the Code of Conduct. The decision about damage done by your post rests with your employer.
- Do not use social media to complain about your agency's actions or policies. If you wish to complain, use your agency's official complaints processes.

Strategies for agencies to prevent misuse

Official use

- Official use of social media is governed by a whole of government policy: the QGCIO *Principles for the official use of social media networks and emerging social media* (December 2015). This contains the guiding principles for supporting a consistent Queensland Government approach to social media for a range of benefits for customers, the community and government.
- The agency should have clear and comprehensive policies and processes so that only authorised/official statements are released.
- There must be a clear process for creating, editing and approving the content of official on-line messages, and limited access to "official" sender accounts to ensure that only approved messages are uploaded or distributed.
- Agencies should immediately remove system access and other access tokens when employees, contract staff and third party service providers cease employment with your organisation.
- Departing employees should sign a separation agreement in which they agree to maintain confidentiality of agency information after they leave.

Personal use

- For personal use, public officers are bound by their agency's Code of Conduct and any agency policies relating to ICT use.
- For public service agencies, the Code (4.3) and the agency's policies address inappropriate use of ICT devices, and the Code (1.3) and the agency's policies address inappropriate public comment.
- Public sector entities should ensure that their Code of Conduct makes appropriate provision to address the making of unauthorised statements during private use of social media, which is supported by relevant policies.
- The Queensland Government Chief Information Office (QGCIO) guidelines and policy document, *Personal use of social media guideline (Dec 2015)* has been developed to assist public service agencies achieve best practice in addressing the personal use of social media where use may impact on an employee's public sector role. It is also recommended guidance for all other public sector organisations.
- Organisations are required to give employees access to education and training[4] about public sector ethics, and their Code of Conduct. This should include information that all social media comments are public, and thorough guidance about what employees can say where.

4 The *Public Sector Ethics Act 1994*. ss. 12K and 21

- Training and information should also cover complaints processes so that staff feel confident that they have a valid internal pathway to discuss issues that trouble them.
- The Code of Conduct places an overriding obligation on all employees to refrain from making inappropriate comments on social media on work matters during personal time or work time on any device or account, whether these are privately or publicly owned. It is further recommended that no comment be made on any work matters, because any comment might attract unwanted attention or be taken out of context.
- Disciplinary action may be taken against employees for any breach of their Code of Conduct. This is made possible by the legislation under which they are employed.

Personal use of official ICT facilities

- Most agencies have a policy which permits limited and reasonable personal use.
- To reduce the risk of misuse, some agencies block access to social media technologies. Others have a policy that permits limited, reasonable personal use based on the Queensland Government's Information Standard 38 – Use of ICT services, facilities and devices. In this case, the onus is on supervisors to ensure that the policy is complied with.

Monitoring and compliance

- Make, maintain and protect all public records in accordance with the *Public Records Act 2002*.
- Ensure employees are aware of the consequences (disciplinary and legal action) related to failing to comply with policies, procedures and legislation.
- Ensure there is a good internal reporting system to help identify and prevent breaches.
- Establish sound risk management strategies and practices, which encompass methods relating to identifying risk areas.
- Record and report all actual and attempted breaches of official policies and of the Code of Conduct.
- Promptly identify, report and rectify any weakness in protocols and procedures to prevent further breaches.
- Encourage self-assessment by employees in relation to their practices.
- Implement methods of monitoring any breaches of electronic security.
- Regularly review protection systems to identify any limitations in these systems in combating wrongdoing from both internal and external threats.

Further information and resources

- *Code of Conduct for the Queensland public service*
- *Crime and Corruption Act 2001*
- *Electronic Transactions Act 2001*
- *Local Government Act 2009*
- *Public Records Act 2002*
- *Public Service Act 2008*

- Australian and International Standard 15489 Records Management
- Code of Ethical Standards, Legislative Assembly of Queensland 2004
- Crime and Corruption Commission: Advisory: Information security and handling
- Office of the Information Commissioner Queensland
- Queensland State Archives Recordkeeping
- QGCIO < www.qgcio.qld.gov.au >
  - Principles for the official use of social media networks and emerging social media
  - Personal use of social media guideline
- Queensland Government Information Security Classification Framework
- Queensland Government Information Standard 18: Information security
- Queensland Government, Information Standard 31: Retention and disposal of public records
- Queensland Government, Information Standard 38: Use of ICT services, facilities and devices policy
- Queensland Government, Information Standard 40: Recordkeeping
- Queensland State Archives website
- Right to Information and Privacy Unit, Department of Justice and Attorney-General

All Queensland legislation is available at www.legislation.qld.gov.au

Crime and Corruption Commission
QUEENSLAND

Please contact us if you would like further detailed guidance and information on any aspect of this advisory.

Crime and Corruption Commission

Level 2, North Tower Green Square
515 St Pauls Terrace, Fortitude Valley QLD 4006

GPO Box 3123, Brisbane QLD 4001

Phone: 07 3360 6060 (Toll-free outside Brisbane: 1800 061 611)

Fax: 07 3360 6333

Email: mailbox@ccc.qld.gov.au

www.ccc.qld.gov.au

Stay up to date

Subscribe for news and announcements:
www.ccc.qld.gov.au/subscribe

Follow us on Twitter:
@CCC_QLD