Queensland Government Enterprise Architecture

Personal use of social media guideline

Final

December 2015

V2.0.1

PUBLIC



Document details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1. **Security classification** | 1. Public | | | | | |
| 1. **Date of review of security classification** | 1. December 2015 | | | | | |
| 1. **Authority** | 1. Queensland Government Chief Information Officer | | | | | |
| 1. **Author** | 1. Queensland Government Chief Information Office and Public Service Commission | | | | | |
| 1. **Documentation status** |  | 1. Working draft |  | 1. Consultation release | 1. 🗹 | 1. Final version |

Contact for enquiries and proposed changes

All enquiries regarding this document should be directed in the first instance to:

Queensland Government Customer and Digital Group  
[qgea@qld.gov.au](mailto:qgea@qld.gov.au)

Enquiries about the management of employee conduct should be directed (via the department’s human resource area) to the Conduct and Performance Excellence service of the Public Service Commission: [cape@psc.qld.gov.au](mailto:cape@psc.qld.gov.au)

Acknowledgements

This version of the *Personal use of social media guideline* was developed and updated by Queensland Government Chief Information Office and the Public Service Commission.

Feedback was also received from a number of agencies, which was greatly appreciated.

Copyright

*Personal use of social media guideline*

Copyright © The State of Queensland (Department of Science, Information Technology and Innovation) 2015

Licence

[](http://creativecommons.org/licenses/by/4.0/)

This work is licensed under a Creative Commons Attribution 4.0 International licence. To view the terms of this licence, visit <http://creativecommons.org/licenses/by/4.0/>. For permissions beyond the scope of this licence, contact [qgea@qld.gov.au](mailto:qgea@qld.gov.au).

To attribute this material, cite the Queensland Government Customer and Digital Group.

Information security

This document has been security classified using the Queensland Government Information Security Classification Framework (QGISCF) as PUBLIC and will be managed according to the requirements of the QGISCF.

Contents

[1 Introduction 4](#_Toc438458954)

[1.1 Purpose 4](#_Toc438458955)

[1.2 Audience 4](#_Toc438458956)

[1.3 Scope 5](#_Toc438458957)

[1.4 QGEA domains 5](#_Toc438458958)

[2 Background 6](#_Toc438458959)

[2.1 What is social media? 6](#_Toc438458960)

[3 Considerations for personal use of social media 6](#_Toc438458961)

[3.1 Authorisation of personal use via government ICT 6](#_Toc438458962)

[3.2 Guidance for employees 9](#_Toc438458963)

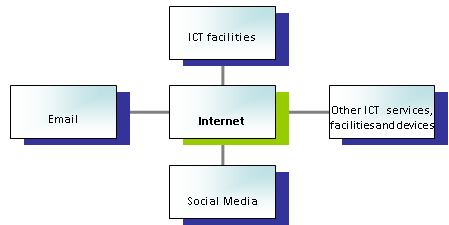
[Appendix A Employee checklist 12](#_Toc438458964)

# Introduction

## Purpose

A Queensland Government Enterprise Architecture (QGEA) guideline provides information for Queensland Government departments on the recommended practices for a given topic area. Guidelines are intended to help departments understand the appropriate approach to addressing a particular issue or doing a particular task. This guideline must be considered by, but does not bind departments.

The [Use of ICT services, facilities and devices policy (IS38)](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/use-of-ict-services-facilities-and-devices-implementation-guideline) provides the authority to a department’s chief executive officer to authorise limited personal and professional use of the internet via Queensland Government ICT services, facilities and devices for departmental employees. Social media web sites are a category of web site/tool which users of the internet will have access to, unless a department specifically blocks such access. This guideline specifies the suggested conditions of personal and professional access to social media web sites via Queensland Government ICT services, facilities and devices where such access has been authorised and should be read together with IS38. It also provides guidance to agencies on engaging with and supporting their employees in the safe and appropriate personal use of social media, whether via Government ICT services, facilities and devices or personal devices.



## Audience

This document is *primarily* intended for:

* chief executive officers/other senior officers who authorise how departmental ICT services, facilities and devices may be used
* human resource professionals
* information management/ICT policy staff.

Departments are responsible for the on-sharing of relevant information with their employees.

## Scope

### In scope

This guideline applies to the personal use of social media whether via Government ICT services, facilities and devices or personal devices, where use may impact on an employee’s public sector role.

### Out of scope

Official use of social media is outside the scope of this guideline and should be distinguished from limited personal and professional use of social media via government-owned ICT services, facilities and devices. Official use of social media is any use of a Queensland Government-managed social media account, profile or presence by an authorised user. Comments made through official social media accounts are representative of the department and made by those authorised to do so. For example, some uses can include; publishing messages, uploading content (text, images, video) and responding to communication from others. For further information, please refer to the QGEA Principles or the official use of social media networks and emerging social media (link to be added once approved). Should an employee receive a message via a private social media account that is official government business they should follow the [Private email use policy](https://www.forgov.qld.gov.au/employment-policy-career-and-wellbeing/directives-policies-circulars-and-guidelines/private-email-use-policy).

### Summary of applicable instruments

QGEA (incl. this guide)

[Use of internet and email policy](https://www.forgov.qld.gov.au/employment-policy-career-and-wellbeing/directives-policies-circulars-and-guidelines/use-of-internet-and-email-policy)

Agency policy

*Public Sector Act 2022* (or employing legislation)

QGEA (incl. Official Use of Social Media Guideline) Code of Conduct

Agency policy

*Public Sector Act 2022* (or employing legislation)

QGEA (incl. this guide)

*Public Sector Act 2022* (or employing legislation)

Agency policy

QGEA (incl. Official Use of Social Media Guideline)

[Private email use policy](https://www.forgov.qld.gov.au/employment-policy-career-and-wellbeing/directives-policies-circulars-and-guidelines/private-email-use-policy)

Code of Conduct

Agency policy

*Public Sector Act 2022* (or employing legislation)

**Platform**

**Personal**

**Official**

**Govt. ICT**

**Personal devices**

**Use**

## QGEA domains

This guideline relates to the following domains:

|  |  |
| --- | --- |
| **Classification framework** | **Domain** |
| Business process | BP-2.4 Develop organisational regulation  BP-8 Develop and manage human resources  BP-9 Manage information and technology resources  BP-11 Manage legislative obligations  BP-11.7 Manage legal and ethical issues |

# Background

## What is social media?

Social media is an umbrella term covering websites, technology, applications or tools that enable active and participatory publishing and interaction between individuals over the internet.

Social media can be characterised by:

* relationships
* user participation
* user-generated content
* collaboration
* multi-directional conversations
* highly accessible and scalable publishing
* 24/7/365 operation and availability.

Employee personal use of social media may be for purely social purposes and/or for professional (career/networking/development) purposes.

# Considerations for personal use of social media

This section of the guide deals with two issues:

* considerations for agencies in deciding whether to authorise personal use through government ICT services, facilities and devices
* guidance on matters agencies should educate their employees about, whether personal use occurs through government ICT services, facilities and devices or using personal devices.

## Authorisation of personal use via government ICT

Departments are encouraged to consider both the risks and the benefits that can be realised from authorising personal use of social media through government ICT services, facilities and devices.

### Benefits

Authorising employee’s limited personal and professional use of social media has been acknowledged as a benefit by some organisations.

#### Professional benefits

The Australian Government’s Government 2.0 Taskforce acknowledged the huge opportunity that online engagement through social media websites offers to advance their mission and boost the professional capability of their staff. Specifically the taskforce stated:

*Generally, engaging with the tools and platforms of social networking should be accepted as a valuable and productive way for public servants to share and develop their expertise. In that sense, they should be accepted as an integral part of their professional development toolkit.[[1]](#footnote-2)* *For instance a public servant may be engaging in social networks, discussing both private and professional matters. Keeping their social connections with other professionals — including from other countries — enhances their network of contacts and possibly enables them to improve their performance.*

In addition, social media websites can assist employees to:

* both share and further develop their expertise
* access useful information sources
* connect with customers and colleagues[[2]](#footnote-3)
* generate ideas for social applications and sites to serve customers[[3]](#footnote-4).

#### Personal benefits

Historically, there has been resistance to new technologies, from the introduction of telephones to email and instant messaging, and while these technologies are now commonplace, they all originally dealt with the same concern - that employees will exploit them for personal use.

It has been found that employees who are encouraged to participate on social media not only revive the company’s external image, but can enable employees to feel ‘empowered, engaged, and proud of where they work’[[4]](#footnote-5).

Other benefits can include:

* an alternative mechanism for organisational communication particularly for business continuity
* building organisational culture
* reducing siloed behaviour.

### Risks

The following table[[5]](#footnote-6) explains some of the risks associated with authorising limited personal and professional use of social media and possible management strategies.

| **Risk** | **Description/example** | **Management** |
| --- | --- | --- |
| Staff productivity | Staff may spend work time on social media | 1. This risk is not unique to social media and applies to the use of any government-owned ICT services, facilities and devices. 2. This risk can be managed by implementing the key requirements of IS38. For information refer to the [IS38 implementation guideline](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/use-of-ict-services-facilities-and-devices-implementation-guideline). |
| Malware and spyware | Social media may pose a greater risk for malware and spyware. | This risk is not unique to social media, and applies to other high traffic sites. Implementation of information security controls can mitigate this risk. |
| Reputation/ legal liability | 1. Public comments made by employees could be construed as official Queensland Government statements. | 1. This risk can be managed by implementing the key requirements of IS38 (see staff productivity above). 2. Departments may also choose to allow the making of limited public comments via government-owned ICT services facilities and devices only in the context of limited professional use. See further appendix A. |
| Publication of personal or confidential information | 1. An employee may publish personal information about another or disclose confidential government information on social media. | 1. This risk is not unique to social media and can be managed by implementing:  * the key requirements of IS38 * mandatory principle 3 of [Information standard 18: Information security responsibilities](https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-digital-tools-and-resources/information-standard-18-information-security-responsibilities) * education for staff on their privacy obligations. |
| Loss of control of published information | 1. Information published on social media is bound by the terms of service or technical limitations of that social media. It may not be possible to remove content that has been published. For example, Jane Smith posts an embarrassing image of a work colleague at a social function on a social media web site. Even though Jane deletes the post a couple of weeks later, the social media has already archived the image. In addition before Jane deleted the image, someone external to government has seen the picture, lifted the image and published it elsewhere. | 1. This risk can be managed by implementing the key requirements of IS38 (see staff productivity above). See also further appendix A. |

## Guidance for employees

Departments should ensure they have strategies in place for promoting awareness among employees of their obligations when using social media (whether on government or personal devices), including the application of the [Code of Conduct for the Queensland Public Service](https://www.forgov.qld.gov.au/employment-policy-career-and-wellbeing/public-service-values-and-conduct/public-service-code-of-conduct) and the conduct, performance and discipline provisions of applicable employing legislation:

*Employees need to be mindful of the way in which they engage via social media and the information they post. Employees should be aware that posting content that reflects seriously and adversely on the public service could give rise to discipline proceedings under the Public Sector Act (PSA) (or applicable employing legislation). This includes (but is not limited to) posts that adversely impact on the public’s confidence in the employee’s ability to do their job impartially and effectively, or that significantly impact on working relationships.*

The below sections provide information agencies should consider incorporating into their policies to give appropriate guidance and support to employees. Examples, relevant to the agency’s operating and service context, should also be considered for inclusion in policy and/or training material.

### Considerations for personal use

When choosing to use media in a personal capacity, employees should ask themselves a number of questions to help make the social media experience a positive one.

* Who can see what I’m posting and do I want them to know this information?

Work email addresses generally should not be used to register for, subscribe etc. to social media sites. Limited exceptions may apply when an employee is using social media to connect to a professional network.

Employees should note that generally under social media sites’ terms of service, potentially all the material posted becomes public information, and can be freely accessed and used by others, and the material becomes the property of the networking host; the employee no longer has control over what is used and where, when or how it is used.

Employees are encouraged to monitor the terms and conditions of the social media platforms that they use on a regular basis, and make sure they are comfortable with privacy settings (if any) applied to their account. Employees should also be mindful that even with privacy settings applied, other users can take screenshots of their posts and repost and share to larger audiences.

* Am I identifiable as a Queensland Government employee?

When using social media employees may be identifiable as a Queensland Government employees, whether or not they explicitly refer to their employment, or even when they post (or respond to a post) under an alias. Employees can be identified as public servants for a number of reasons, including as a result of the nature of the information they post or because members of their social media networks may already be aware they are public servants.

It is important that other users understand when a comment/view etc. is expressed by an employee (including endorsing or ‘liking’ another’s post), it is the employee’s personal opinion, particularly where the view expressed is not an endorsed government position or inconsistent with their departments/government position. Employees may consider including a disclaimer that the opinions expressed are their own and not those of their employer, however such a statement does not absolve the employee of the obligation to ensure their comments do not reflect seriously and adversely on the public sector.

Tips:

* employees should remember social networking sites such as Facebook and LinkedIn may display their specific details about their employment on their profile page
* where possible, Queensland Government employees should generally use personal email addresses to register and log into personal accounts. There are exceptions, for example, Yammer requires an organisational email address to register.
* should an employee receive a message via a private social media account that constitutes official government business they should follow the [Private email use policy](https://www.forgov.qld.gov.au/employment-policy-career-and-wellbeing/directives-policies-circulars-and-guidelines/private-email-use-policy).
* How am I conducting myself on social media, and how does this impact on others, including my employer?

Employees need to be mindful of the way in which they engage via social media and the information they post. Employees should ask themselves:

Are my posts polite and respectful (including about colleagues, stakeholders etc.) and consistent with the terms of use of the relevant social media platform/website, as well as other applicable laws (e.g. copyright, anti-discrimination etc.)?

Am I only disclosing and discussing publicly available information and ensuring my posts are accurate and not misleading?

Do I have a conflict of interest with the topics discussed and my official role?

Have I obtained consent before using the identity or likeness (including photographs) of another employee, contractor or other member of the agency?

How will my post reflect on the public service? Could my post be grounds for discipline?

Whether posts made by other people on my page are inappropriate, and if so, need to be deleted?

### Staying safe on social media

While most people who use social networking sites are well intentioned, employees need to be careful about the information they share and how to protect it. People can inadvertently or intentionally use other people’s personal information to embarrass or damage their reputation, or even steal their identity. Some tips are set out below and a sample checklist for employees is available at Appendix A.

* Privacy and security settings exist for a reason: Learn about and use the privacy and security settings on social networks. They are there to help you control who sees what you post and manage your online experience in a positive way.
* Once posted, always posted: Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn’t want your parents, colleagues or employer to see. Research has found that 70% of job recruiters rejected candidates based on information they found online[[6]](#footnote-7).
* Keep personal information personal: Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may be for a hacker or someone else to use that information to steal your identity, access your data, or commit other crimes such as stalking.

Strategies for managing these risks include avoiding identifying your place of work on personal social media sites and not using GPS tracking functionality to ‘check-in’ to your place of work.

Common sense and discretion must be used when posting work-related content (including official travel for work purposes, or when representing their agency in an official capacity) on personal social media accounts.

* **Know and manage your friends**: Carefully consider who should be granted access to your social media accounts (e.g. when adding ‘friends’ on Facebook or permitting access to Flickr photograph albums).Use tools to manage the information you share with different groups.
* **Be honest if you’re uncomfortable**: If a colleague posts something about you that makes you feel uncomfortable or you think is inappropriate, if you feel comfortable in doing so, let them know. You can also discuss concern with your supervisor or human resource area. Likewise, stay open-minded if a colleague approaches you because something you have posted makes him or her uncomfortable.
* **Know what action to take**: If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. You can also raise concerns with your supervisor or human resource area if the person engaging in the concerning behaviour is also a public servant.

You can view more tips at Australian Government [Stay smart online](https://www.digitalhealth.gov.au/newsroom/blogs/five-ways-you-can-stay-smart-online).

1. Employee checklist

Departments may include the following checklist as part of their policies and procedures as a guide for employees when they are posting material on a social media website via government-owned ICT services, facilities and devices.

Employees should ask themselves these questions prior to posting content on social media. If any of an employee’s answers fall within the do not post column, then the employee should not post the material.

|  |  |  |
| --- | --- | --- |
| **Question** | **Do not post** | **Post** |
| Will the reputation of your department or the Queensland Government be harmed? | Y | N |
| Will your personal or professional reputation be harmed? | Y | N |
| Will the personal or professional reputation of a colleague be harmed? | Y | N |
| If the posting contains the personal information of another person, do you have their consent to post that information? | N | Y |
| In posting the material, are you behaving with integrity, honesty, respect and accountability? | N | Y |
| Is it clear to others that you are making the posting as a private individual and not as an authorised representative of your department or the Queensland Government? | N | Y |
| Does the posting contain inappropriate or offensive material? | Y | N |
| Does the posting contain confidential information that is not already in the public domain? | Y | N |
| Does the posting contain information about your official role and duties, or work related activities or events, that are not already in the public domain? | Y | N |
| Does the posting give the impression that you are the authorised representative of your department or the Queensland Government or that your personal opinion is the opinion or position of your department or the Queensland Government? | Y | N |
| Are you willing to accept the posting as a permanent and public record of your personal opinion? | N | Y |
| Would you be willing for the content of your posting to be viewed by a stranger on the street or your supervisor? | N | Y |
| Does the posting otherwise constitute an unauthorised use of Queensland Government ICT services, facilities and devices? | Y | N |

1. Australian Government, Department of Finance and Deregulation, Australian Government Information Management Office, *Engage: Getting on with Government 2.0, Chapter 4: Promoting online engagement,* available at<http://www.finance.gov.au/publications/gov20taskforcereport/chapter4.htm>, accessed 29 April 2011. [↑](#footnote-ref-2)
2. Berhnoff, J. & Schadler, T. *Empowered: Unleash your employees, energize your customers, transform your business,* Harvard Business Review, Boston, 2010, p. 129. [↑](#footnote-ref-3)
3. See 3. [↑](#footnote-ref-4)
4. <http://www.prdaily.eu/PRDailyEU/Articles/Can_GM_employees_woo_the_country_back_through_soci_5277.aspx> [↑](#footnote-ref-5)
5. Government of South Australia, *Social media guidance for departments and staff,* available at <http://www.espi.sa.gov.au/files/socialmedia_guidelines.pdf>, accessed 19 May 2011; Victorian Government, *VPS Gov 2.0 Risk Register and Management Plan,* available at <http://www.intranet.vic.gov.au/sites/default/files/Gov%202.0%20Risk%20Management%20Plan.XLS>, accessed 19 May 2011. [↑](#footnote-ref-6)
6. *The web means the end of forgetting*, Rosen, J,The New York Times, 21 July 2010. [↑](#footnote-ref-7)