Social Media

Employee Acceptable Use Policy

Overview

The Department of Infrastructure & Transport (the Department) recognises that there are legitimate business and personal reasons for using social media at work or using corporate computing resources. To enable employees to take advantage of the business value of these sites and to promote an open, trusting, collaborative workplace, the Department policy allows employees to use social media within the guidelines specified below.

What is Social Media?

Social media includes any web site in which visitors are able to publish information to a larger group. Information shared may include (but is not limited to) personal information, opinions, research, commentary, or business information. Examples of such destinations include large branded entities such as Facebook, Twitter, YouTube, and LinkedIn. However, blogs, special interest forums, user communities are also considered social media.

Inappropriate Content

While social media contains legitimate business and personal content, it may also include content that is offensive, obscene, pornographic, sexually suggestive, abusive or discriminatory defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringing copyright or is otherwise unlawful. Therefore, the same inappropriate content policy that applies to the broader web and email, also applies to content found within social media.

Inappropriate content must not be accessed by employees while at work, or while using Departmental resources. Likewise, staff must not post inappropriate material using Departmental resources. Employees are expected to use common sense and consideration for others in deciding which content is appropriate for the workplace.

Productivity

The Department recognises that employees have a need, at times, to conduct both official and personal business within social media while at work or using Departmental resources. Therefore, the Department allows limited access to non-business social media content. For example, employees are allowed to access personal communications applications, email, and blog content within social media which is based on a quota time allocation. It is the responsibility of the employee to ensure that personal use is consistent with the Departments' guidelines on the *Code-of-Conduct for the use of Email and Internet services*.

Content Publishing and Classified Information Policy

Content Publishing and Classification Guidelines

The following are policy guidelines regarding what you should and should not do when publishing content in social media. Employees are responsible for content they publish in social media and can be held personally liable for content published. Employees can also be subject to disciplinary action by the Department for publishing inappropriate or classified content. These guidelines only cover a sample of all possible content publishing scenarios and are not a substitute for good judgment.

It is important to note that these guidelines apply to all social media publishing whether personal or Department-sponsored.

When accessing social media via the Department's internet, intranet systems, you must do so in accordance with the Department's *Code-of-Conduct for the use of Email and Internet services*, which requires you to use these resources 'reasonably', in a manner that does not interfere with your work, and is not inappropriate or excessively accessed.

Personal use of social media

The Department recognises that you may wish to use social media in your personal life. This policy does not intend to discourage nor unduly limit your personal expression or online activities.

However, you should recognise the potential for damage to be caused (either directly or indirectly) to the Department in certain circumstances via your personal use of social media when you can be identified as a Departmental employee. Accordingly, you should comply with this policy to ensure that the risk of such damage is minimised.

You are personally responsible for the content you publish in a personal capacity on any form of social media platform. When in doubt, you should seek guidance from the Department on how to comply with the following obligations.

Personal Posts

Personal Posts are those made via a private social media account in your name or a name of your choosing. It is not recommended that personal accounts identify officers as working for the Department, however it is noted that in the cyber sphere it can be relatively easy for people to connect separate pieces of information to largely identify users.

Use of Personal Posts should follow similar considerations as the use of email, and not disclose information that would otherwise not be disclosed, speculate on policy or possible policy, or indicate possible future decisions of the Government.

Personal social media accounts should not be linked to Departmental email accounts.

If you feel that you could be easily identified as an officer of the Department it is recommended a disclaimer be used – see *Dos and Don'ts* section below.

Where you can be identified as a Departmental Officer

Do not disclose information that would otherwise not be disclosed, speculate on policy or possible policy, or indicate possible future decisions of the Government.

Ensure that all content you publish is accurate and not misleading.

State on all postings (identifying you as a Government employee) the stated views are your own and are not those of the Department or the Government and do not imply that you are authorised to speak as a representative of, or on behalf of, the Department or the Government.

Maintain the standard of professionalism expected in your role.

Do not publish material that could harm the reputation of the Department or Government (including officials, elected Ministers/Members/Senators, or their staff), stakeholders or clients.

Adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

Do not use your Department email address or Government logos/identifiers.

Do not use or disclose any confidential information or personal information.

Do not post material that is, or might be construed as, threatening, harassing, bullying or discriminatory towards another employee/contractor of the Department, or towards clients or stakeholders.

Do not post images or footage of colleagues without their permission.

Do not post any material that might cause damage to the Department's reputation or bring it into disrepute.

Professional Posts

Professional use of social media is based on your area of expertise and/or association with other practitioners in that field. Some employees are subject matter experts in fields that may relate to their employment in the Department, or may be wholly separate from it, and might make comment in that capacity.

An employee's manager should be made aware of any sites or accounts an employee holds that may reasonably reflect on their employment in a professional capacity at the Department. This includes formally blogging or hosting accounts on issues relevant to their area of professional expertise. The employee should also make it clear when making public comment in that role that they are not representing the Department or the Government.

Official and Authorised Use

Official Posts

The Department reserves the right to make Official Posts on social media sites, as it does in the traditional media, to address queries, discussion and misinformation. Any Official Posts will identify the information provided as attributable to the Department as official comment.

Official Posts will be executed by a fully authorised representative.

As with any public statements any official posts must be developed in-conjunction with the Communications Branch, subject matter experts and the appropriate SES Officer.

Care should be taken when considering official posts as social media is an open and dynamic environment which can generally not be controlled – consider the potential implications of any proposed posts, the likely audience, and whether it will assist in delivering outcomes for the Department and Government.

If at any time the Department chooses to make official comment via social media this will be managed by Corporate Services in conjunction with the subject matter area(s).

Official Posts are also required to follow the Department's *Media Protocols*.

Australian Public Service Commission circular 2012/1 provides information on Whole-of-Government protocols on making public comment and participating online.

Authorisation to Represent the Department in Social Media

Before engaging in social media as a representative of the Department, you must become authorised to comment.

You may not comment as a representative of the Department unless you are authorised to do so.

Only those persons officially designated by the Department have the authorisation to represent the Department on employee sponsored social media pages or other social media pages. If and when staff engage in advocacy for the Department and have the authorisation to participate in social media, they should identify themselves as such.

Authorisation to represent the Department in social media must be sought from and granted by the relevant Executive Director.

While the Department allows personal use of social media, social accounts should not be used to convey official posts, and staff should take due care that the use of social media does not impinge on performing their work or be used excessively.

Malware and Online Crime Prevention

Social media is commonly used by the online criminal community to deliver malware and carry out schemes designed to damage property or steal classified information. While these guidelines help to reduce risk, they do not cover all possible threats and are not a substitute for good judgment.

Security setting, applications and common sense should be used when using social media. For tips see the – see *Dos and Don'ts* section below, or contact the Department's IT Security Adviser.

Do's and Don'ts

Do	Do Not
Follow the policies. Make yourself aware of and follow all Departmental privacy and classification guidelines. All guidelines, as well as laws such as copyright, fair use and financial disclosure laws apply to social media.	**Do Not** use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in the Department's workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory.
Be professional. If you have identified yourself as a Departmental employee within a social website, you are connected to your colleagues, managers and even the Departments' customers. You should ensure that content associated with you is consistent with your work at the Department.	**Do Not** conduct classified business with a stakeholder or client through your personal or other social media.
Ask permission. to publish or report on conversations that are meant to be private or internal to the Department and when in doubt, always ask permission from the Department's Communications Branch or legal section.	**Do Not** register accounts using the Departments' brand name or any other unregistered or registered trademarks.
Speak in the first person. (I , Me) when engaging in personal social media communications. Make it clear that you are speaking for yourself and not on behalf of the Department.	**Do Not** use the same passwords for social media that you use to access Departmental computing resources.
Use a disclaimer. If you publish personal social media communications and it has something to do with the work you do or subjects associated with the Department, use a disclaimer such as this: "The postings on this site are my own and don't necessarily represent those of the Department."	**Do Not** follow links on social media pages posted by individuals or organisations that you do not know.
Link back to the source. When you do make a reference to a stakeholder, where possible link back to the source.	**Do Not** disclose or use the Department's classified or sensitive information or that of any other person or company. For example, ask permission before posting someone's picture in a social network or publishing in a blog a conversation that was meant to be private.
Be aware of your association with social media. If you identify yourself as a Departmental employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.	**Do Not** download software posted or recommended by individuals or organisations that you do not know.
Note activity is logged. Be aware that the Department employs technical controls to provide reminders, allow auditing and enforce these guidelines.	**Do Not** comment on Departmental or Government business.
For IT security use a security application to protect personal social media pages and configure social media accounts to encrypt communications whenever possible. Facebook, Twitter and others support encryption as an option. If any content you find on any social media web page looks suspicious in any way, close your browser and do not return to that page.	**Do Not** cite or reference stakeholders without their written approval.