QUESTION TAKEN ON NOTICE

SUPPLEMENTARY BUDGET ESTIMATES HEARING: 17 OCTOBER 2011

IMMIGRATION AND CITIZENSHIP PORTFOLIO

(SE11/0018) Program: Internal Product

Senator Hanson-Young (L&CA 45) asked:

Provide a copy of the protocol for the use of social media (particularly in relation to the use of Twitter) by departmental staff.

Answer:

Attached is the Department of Immigration and Citizenship's social media policy which outlines the protocols in relation to the use of social media by departmental officers.

Use of social media in the Department of Immigration and Citizenship

Purpose

The purpose of this section is to provide guidance for all Department of Immigration and Citizenship employees and contractors on the use of social media tools.

What are social media tools for online communication?

Social media include a range of new tools and technologies. The following list is not exhaustive nor does it cover all platforms:

- Blogs—an online journal of opinions, brief paragraphs and information that can be updated regularly.
- Wikis—web-based systems for generating web pages, allowing users to collaborate by adding, removing and editing content collectively.
- Podcasting—created by posting an audio file to a website which can then be downloaded via subscription.
- RSS (Really Simple Syndication [RSS]—allows users to receive updated information from websites, blogs or podcasts without having to visit a website repeatedly. RSS provides open and timely communication about specific issues to its various audiences.
- Social bookmarking—refers to group-based collections of links to articles and media. Users bookmark links to the web pages they want to remember or share.
- Tagging—relates to keyword classification of content carried out by users which in turn yields more relevant and useful categorisation and search results.
- Social networking sites such as Facebook, LinkedIn, My Space and Flickr—provide users with infrastructure and resources to connect and communicate with each other and share and exchange content.
- Mash-ups—a web service that pulls together data from different sources to create a new service or product. Mash-ups take information typically stored in separate software applications and combine them into new hybrid applications.
- Virtual worlds (such as Second Life)—allow users to create a physical online identity and socialise with each other, create objects and buildings and conduct sales.

Official use of online communication tools

All online communication on behalf of the department must be authorised. The process for doing this will depend on the nature and purpose of the communication.

Working with online media in an official capacity is subject to the same standards required by the *Public Service Act 1999* (APS Values and the APS Code of Conduct) that apply in a physical work environment. These include:

- behaving honestly and with integrity
- not providing false or misleading information in response to a request for information that is made for official purposes in connection with APS employment

- dealing appropriately with information, recognising that some information needs to remain confidential
- being apolitical, impartial and professional
- delivering services fairly, effectively, impartially and courteously to the Australian public
- behaving with respect and courtesy, and without harassment
- being sensitive to the diversity of the Australian public
- taking reasonable steps to avoid conflicts of interest
- making proper use of Commonwealth resources
- upholding the APS Values and the integrity and good reputation of the APS.

DIAC employees making official use of online media must:

- comply with the department's email and internet instruction and DIAC Code of Conduct guidelines
- declare the purpose of the communication and their position as a representative of the department, unless there are exceptional circumstances such as a potential threat to personal security
- avoid any statement or comment that might bring the department, the government or the APS into disrepute
- be accurate and impartial and avoid any comment that could be interpreted as a political view
- do not commit the department or the government to any action or initiative without appropriate authority
- do not disclose official information unless you are authorised to do so or unless it is already in the public domain
- be aware of laws covering libel, defamation, privacy and the protection of intellectual property
- avoid the risk of liability for the department by not providing recommendations or referrals for friends and or associates
- ensure the terms and conditions of use do not conflict with APS or departmental policies
- avoid any statements that might be interpreted as advocating government policies or criticising the policies of other political parties or groups
- be aware that people online may mask their real identity
- protect personal information such as identity documents, drivers licence, banking and financial information from distribution in the public domain
- understand how to use privacy settings and preferences to restrict access to content
- obtain prior permission to use words, images or materials for online communications.

The department will establish systems for ensuring that online communication is consistent with information and advice being provided by the agency through other media and fora. Information and views expressed should be accurate, clear and not open to ready misrepresentation

Confidentiality and proprietary information

Before using a social networking site, employees should ensure there is no conflict for the department in complying with the owner's Terms of Service.

Potentially, all content posted to social networking sites becomes:

- public information freely available to those who access it
- information that can be used as source material for journalists and other interested parties, and
- the property of the networking host.

Employees who engage in social networking from work can be identified by their email address. Basic operational and personal security considerations must be applied at all times.

Personal use of social networking sites

The Australian Public Service Commission (APSC) has issued Circular no. 2009/6: protocols for online media participation. The principles of the protocols derive from the APS Values and the APS Code of Conduct.

Departmental staff should be aware that using public social networking sites, blogs, video portals or wikis carries the risk of identity fraud and other threats which can result from providing personal information on such sites, specifically details such as age, address and employment details.

Employees who blog in their own time using their own resources should not record any information regarding their employment, including work email address, contact lists, work duties or any photographs of DIAC employees at work-related functions and activities after hours or while away from home.

Employees should also consider potential consequences for safety and security before listing any personal details relating to themselves, their colleagues and family members on the internet.

The following chart provides general guidance for staff using online media.

Official use of online communication	Do not
Do be aware that employees who engage in social networking from work can be identified by their email address. Unless there is a potential threat to personal security, declare the purpose of your communications and your position	Do not use work email address or contact lists when registering on social media sites.
Uphold the APS Values and Code of Conduct and behave at all times in a way that upholds the values, integrity and good reputation of the APS.	Do not post material on line that may compromise the interests and reputation of the government or the department.
Do be aware that you may be identified as having a perceived or real conflict of interest if using departmental information online.	Do not commit the department or the government to any action or initiative without appropriate authority.
Recognise that some information related to the operations of government and the department needs to remain confidential. Operational and personal security considerations must be applied at all times.	Do not disclose information obtained or generated in connection with APS employment if it could potentially be prejudicial to the effective working of government policies and programs.
Be accurate, professional, impartial, apolitical, respectful, and courteous when participating in robust policy conversations.	Do not make any comment that could be interpreted as a political view, or disrespectful or discourteous.
Be aware of the laws covering libel, defamation, privacy and the protection of intellectual property.	Do not make any statement that might harm the reputation of individuals, the government or the department.
Get prior permission in writing from an authorised person before using words, images, links or other material (such as audio and visual content) for online communications.	Do not post photos online—including photos of work-related activities and events or photos containing images related to the department (for example: signs, uniforms, flags, buildings)—without prior permission from a relevant manager and from other people depicted in the photo.
Behave honestly and with integrity at all times.	Do not provide false or misleading information for official purposes in connection with your APS employment.

Personal use of online communication	Do not
Be aware that people online may disguise their real identity. Protect yourself, your family and your colleagues from the risk of identity fraud and other threats.	Do not disclose any personal information, such as age, address, banking and financial information, passport, driver licence and employment details, or information about work related activities and events.
Consider carefully whether you should identify yourself as an APS employee or an employee of the department.	Do not risk any liability for the department by providing online recommendations or referrals for friends and or associates.
If posting photos online that include colleagues or friends, ask them for their permission to include photos in which they appear.	Do not post photos of colleagues or friends online without their permission.
Ensure the terms and conditions of use do not conflict with APS or departmental policies. Content posted online potentially becomes public information and the property of the networking host.	Do not post information or images that may damage your personal or professional reputation or that of your colleagues or family members now or in the future.
Understand how to use privacy settings and preferences to restrict access to content.	Do not expose yourself, your family and friends to the risk of fraud, identity theft and abuse of privacy.