Information Management Advice 57 Sample Social Media Acceptable Use Policy

Overview

The [agency] 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 agency policy allows employees to use social media within the specified guidelines.

Scope

This policy applies to all workplace participants, which include:

- all employees – including casual, fixed term and otherwise temporary employees, employees on probation, part-time employees, managers, employees working from home as well as fulltime and ongoing employees;
- people providing services to the agency on a contract basis or on secondment from or to another agency, even if they are only working on a temporary basis;
- students, graduates and others on work experience or undertaking voluntary work.

What is Social Media?

Social media (sometimes referred to as social networking or Web 2.0 technologies) are online services and tools used for publishing, sharing and discussing information. They can include forums, blogs, wikis, social networking websites, and any other websites that allow individual users to upload and share content.

Social media services and tools can involve a combination of technology, telecommunications and social interaction. They can use a variety of different formats, for example text, pictures, video and audio.

Social media can provide unique opportunities for users to communicate and share information, and to build networks locally, nationally, and internationally. Information shared may include (but is not limited to) personal information, opinions, research, commentary, or business information.

Social Media Examples

Blogs – A blog is a "web log". Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. Usually, viewers can comment, ask questions, share information and subscribe. A typical blog combines text, images, and links.

Forums / boards – An internet forum, or message board, is an online discussion site. Users can post messages and comment on other messages. Other types of social media often incorporate forums, sometimes with their own social conventions and etiquette (or 'netiquette').

Micro-blogs – A micro-blog has a similar purpose to a blog, except that entries are smaller - usually limited to a certain number of characters (e.g. 140). A popular example is Twitter™. It allows users to 'follow' one another so that they are notified when a new update is posted. Users can connect quickly and through many different tools such as their mobile phone.

Photo sharing sites – A photo sharing site, such as Flickr®, allows users to upload images and is useful for categorising and organising pictures. They allow other users to comment on them, or re-use them with permission.

Social bookmarking – Social bookmarking is used for saving the address of a website or item of content and adding a tag to allow other users to easily find your research. It is useful for organising and sharing links, and for keeping track of links recommended by others. Delicious™, Digg™, and Reddit are popular examples.

Social networking websites – Social networking websites focus on building online communities of people who share interests. Popular examples include MySpace™, Facebook® and LinkedIn®. Users can build their own profile page, join groups, share photos and videos, post messages, and run other applications.

Video sharing sites – A video sharing site allows users to upload video clips to be stored on the server, allowing other users to view them. YouTube™ is a popular example.

Virtual worlds – Virtual worlds such as Second Life® are online places where users can create representations of themselves (avatars) and socialise with other residents.

Wikis – A wiki is a website using 'wiki software' that allows web pages to be created, interlinked, and edited by any user. The most well known wiki is Wikipedia® – an online encyclopaedia.

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, hateful, racist, sexist, that infringes 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 [agency] resources. Likewise, staff must not post inappropriate material using agency resources. Employees are expected to use common sense, and consideration for others, when deciding on content appropriate for the workplace.

Productivity

The [agency] recognises that employees may have a need, at times, to conduct both official and personal business within social media while at work or using [agency] resources. Therefore, the [agency] 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 [agency] guidelines on the [insert ‘appropriate use’ policy or other].

Content Publishing and Classification Guidelines

The following are 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 agency 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 agency-sponsored.

When accessing social media via the agency's internet, intranet systems, you must do so in accordance with the agency's [reference appropriate Code-of-Conduct or Acceptable Use policy] 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 agency recognises that you may wish to use social media in your personal life outside of work time. 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 agency in certain circumstances via your personal use of social media when you can be identified as an agency 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 agency on how to comply with the following obligations.

Personal Posts

Personal Posts are those made via a private social media account in your own name, or a name of your choosing. Personal accounts should not identify officers as working for the agency, 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 other agency ICT communication resources (eg. Email, etc), 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 agency email accounts.

If you feel that you could be easily identified as an officer of the agency, it is recommended a disclaimer be used - see Appendix 1 *Dos and Don'ts*.

Where you can be identified as an Agency Officer

Do not disclose information that would otherwise not be disclosed; speculate on policy or possible policy; or indicate possible future decisions of the agency or Tasmanian Government. Ensure that all content you publish is accurate and not misleading.

State on all postings (identifying you as a State or Local Government employee) the stated views are your own and are not those of the agency and do not imply that you are authorised to speak as a representative of, or on behalf of, the agency. Maintain the standard of professionalism expected in your role.

Do not publish material that could harm the reputation of the agency (including officials, elected Ministers/Members, 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, discrimination, harassment and other applicable laws.

Do not use your agency email address or agency 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 agency, 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 agency'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 agency, 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 agency. 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 agency.

Official Posts

The agency 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 agency as official comment.

Official Posts will be executed by a fully authorised representative of the Agency. A list of authorised representatives is maintained by [Communications Branch], and available from the [corporate intranet].

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

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 agency.

If at any time the agency chooses to make official comment via social media this will be managed by the [Communications Branch] in conjunction with the subject matter area(s).

Official Posts are also required to follow the agency's [Communications Policy] and protocols.

Section 8.5 Non-Tasmanian Government websites of the *Tasmanian Government Communications Policy* provides information on Whole-of-Government protocols on making public comment and participating online.[1]

Authorisation to Represent the agency in Social Media

Before engaging in social media as a representative of the agency, you must be formally authorised to comment.

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

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

Authorisation to represent the agency in social media must be sought from and granted by the [Communications Branch] who will update and maintain the agency register of official social media accounts as appropriate.

While the agency allows limited personal use of social media, personal 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 settings, applications and common sense should be used when using social media. For tips see the Dos and Don'ts section below, and/or contact the agency's ICT Manager.

[1] Tasmanian Government Communications Policy

Policy breaches and Non Compliance

Non-compliance and breaches of this policy will be dealt with in accordance with the relevant employment agreement and corporate policy. Allegations of misconduct will be investigated according to established procedures. Sanctions for non-compliance or violations of this policy may include the following:

- Temporary or permanent revocation of access to some, or all, computing and networking resources and facilities;
- Disciplinary action including possible termination of employment or contract; and/or
- Where inappropriate use constitutes a breach of any law, legal action may be taken in accordance with that law by the agency, or concerned third parties.

Related Policies

This policy should be read in conjunction with existing corporate policies including the [Conflict of Interest Policy, Email and Internet Use Policy, Records and Document Management Policy, State Service Principles, relevant Codes of Conduct, and the Workplace Behaviour Policy].

Employee Declaration

I,   , hereby acknowledge that I have read and understand the Social Media Acceptable Use Policy. I agree to abide by the terms and conditions of this policy, and ensure that persons working under my supervision abide by the terms and conditions of this policy. I understand that if I violate or fail to comply with this policy, I may face legal or disciplinary action according to the agency's disciplinary procedures.

________________________________   ________________________________

Employee Signature   Date

________________________________   ________________________________

Manager Signature   Date

________________________________   ________________________________

[Social Media] Program Administrator Signature   Date

Appendix 1 – Social Media "Do's and Don'ts"

DO	DO NOT
Follow the policies. Make yourself aware of and follow all agency privacy and classification guidelines. All guidelines, as well as laws such as copyright, fair use, and disclosure laws apply to social media. Ensure you have read and understood any Terms of Use for the social media platform you intend to use.	DO NOT use ethnic slurs, personal insults, obscenity or engage in any conduct that would not be acceptable in the agency'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 an [agency] employee within a social site, you are connected to your colleagues, managers and the agency's customers. You should ensure that content associated with you is consistent with your work at the agency.	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 agency. When in doubt, always ask permission from the agency's Communications Office, legal section or your manager.	DO NOT register accounts using the agency's brand name, or any other unregistered or registered trademarks.
Communicate in the first person (I, me) when engaging in personal social media communications. Make it clear you are speaking for yourself, and not on behalf of the agency.	DO NOT use the same passwords for social media that you use to access agency 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 agency, use a disclaimer such as "The views expressed on this site are my own, and don't necessarily represent those of the [agency]".	DO NOT follow links on social media pages posted by individuals or organisations that you do not know.
When you do make an (approved) reference to a stakeholder, where possible link back to the source.	DO NOT cite or reference stakeholders without their written approval.

Be aware of your association with social media. If you identify yourself as an [agency] 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 agency employs technical controls to provide reminders, allow auditing, and enforce these guidelines.	DO NOT comment on agency or Government business.
For IT security, use a security application to protect 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 disclose or use the agency'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.
Ensure that appropriate records are captured of official social media account activities, in accordance with the Archives Act, the agency Recordkeeping policy, and where information is unique.	DO NOT utilise (and rely on) social media applications as information repositories. As much as possible, use information that already exists elsewhere in the agency - posting only *duplicate* information to social media sites reduces information management requirements.

Further Advice

For more detailed advice, please contact:

Government Information Strategy Unit
Tasmanian Archive and Heritage Office
91 Murray Street
HOBART TASMANIA 7000
Telephone: 03 6165 5581
Email: gisu@education.tas.gov.au

Acknowledgements

- Commonwealth Department of Infrastructure and Transport Social Medial Employee Acceptable Use Policy.[2]
- South Australian Government, Social Media Guidelines[3]
- ABC, Use of Social Media Policy[4]

Information Security Classification

This document has been security classified using the Tasmanian Government Information Security classification standard as PUBLIC and will be managed according to the requirements of the Tasmanian Government Information Security Policy.

Document Development History

Build Status

Version	Date	Author	Reason	Sections
2.0	May 2015	Christine Woods	Template	All
1.0	May 2014	Allegra Huxtable	Initial Release	All

Amendments in this Release

Section Title	Section Number	Amendment Summary
All	All	Documented imported into new template

Issued: June 2014

Ross Latham
State Archivist

[2] http://www.infrastructure.gov.au/department/ips/files/log/FOI_12_65_document_1.pdf
[3] http://publicsector.sa.gov.au/
[4] http://www.abc.net.au/mediawatch/transcripts/1303_abcsmp.pdf