Appendix B: Risk Assessment Matrix

Sub-category	Description	Consequence rating	Likelihood	Potential platforms effected	Planned mitigation
Strategic: risks that cause campaigns or projects to not deliver aims or objectives.	**Inappropriate choice of social media:** The Office chooses to use or collaborate for engagement with a web 2.0 tool that does not meet communications or business objectives.	Negligible	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	The Senior Communications Advisor and Manager or subject matter expert consider which social media channel/s to use at the planning stage of each communications campaign. Target audiences and objectives are used to assess which social media channel, if any, should be used and what content should be provided.
Reputation: risks that damage stakeholder's perception of the Office.	**Brand damage:** A user contributes content that damages the Office's reputation. Eg. Content that questions the Office's credibility. Or, the Office asks its followers a question on a social media platform and receives an influx of critical comments not directly related to the question.	Minor – moderate (depending on the level of criticism)	Likely	All: Facebook, Twitter, YouTube, Vimeo.	In keeping with our social media guidelines, moderation of all content on the Office's social media channels will ensure inappropriate content is removed—content that may include swearing and defamatory comments. Comments that are critical of the Office will usually remain, as we cannot be seen to censor other people's views or opinions. The Senior Communications Advisor will work with subject matter experts and managers to formulate appropriate responses (if applicable), to rectify the sentiment and our reputation. It should be noted that Twitter cannot be moderated. All tweets are posted on each user's individual profile, and go to their followers. Only posts by @eSafetyOffice will appear on our profile. @eSafetyOffice can remove its own posts, but cannot remove another person's post. If the Office receives a large amount of negative feedback and criticism to a question asked on one of its platforms, we may issue an apology, as well as remove all posts.
	Breach of publication rights: The Office publishes content (or digital assets) that infringes copyright (or agreed/licensed digital rights).	Major	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	All content that is not property of the Office is referenced or linked to the original asset. All planned content will be available in the social media calendar and accessible by Managers to review.
	Breach of implicit trust:	Major	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	Any advice provided on the Office's social media channels will be cleared by subject matter experts before publishing. In keeping with our social media guidelines, moderation of all content on the Office's social media channels will ensure

	Office advice is contrary to public opinion received on an Office web 2.0 platform.				inappropriate content is removed—content that may include swearing and defamatory comments. Comments that are critical of Office advice will usually remain, as we cannot be seen to censor other people's views or opinions. The Senior Communications Advisor will work with the subject matter expert or Manager to formulate an appropriate response (if applicable), to rectify the sentiment and our reputation.
	Hijacking: An Office social media account is hijacked by individuals, industry lobby groups, or special interest groups.	Moderate	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	The Senior Communications Advisor will alert Managers (if appropriate) about the influx of comments from an organised lobby group or special interest group. The Senior Communications Advisor or other appropriate staff member will then endeavour to contact the group to engage with them in another way (eg. private message), that does not continue to disrupt the Office's social media channel or damage the brand's reputation. In keeping with our social media guidelines, moderation of all content on the Office's social media channels will ensure inappropriate content is removed—content that may include swearing and defamatory comments.
	Breach of confidentiality (information privacy): The Office inadvertently releases confidential or private information on one of its web 2.0 services.	Major	Unlikely	Facebook, Twitter	There is strict governance in place over the publishing of sensitive content on the Office's social media channels. Sensitive content will be cleared by a Manager and EM, if appropriate. If confidential content was ever published, the Senior Communications Advisor has control to remove postings immediately from its channels once noticed.
	Information quality and integrity: The Office publishes information that is inaccurate, has been superseded, or lacks integrity or quality.	Moderate	Unlikely	Facebook, Twitter	Any advice provided on the Office's social media channels will be cleared by subject matter experts before publishing. If inaccurate content is ever published, the Senior Communications Advisor will update the content immediately with the correct information, or remove it immediately. The Office will remain honest and transparent about any miscalculations made on social media.
Security: risks that are related to identify theft	**Hacking:** An Office social media account/s is hacked and passwords are changed. Content is no longer controlled by the Office.	Major	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	All of the Office's social media passwords are kept in a locked, master spreadsheet in SharePoint. All passwords use a combination of letters, symbols and numbers that exceed the character minimum. Passwords will be changed at regular intervals and managed by the Senior Communications Advisor. In addition, no staff member will access an Office social media account from their personal mobile phones / tablets / home computers/laptops. An office iPad will be used to

					access social media accounts at external events, containing ACMA security logins. Other ways to secure our accounts are being investigated to provide similar protections as two-factor authentication.
	Fake accounts: A fake Offcie profile is set up on a social media platform, by someone outside the organisation.	Moderate	Unlikely	All: Facebook, Twitter, YouTube, Vimeo and others	The Senior Communications Advisor actively monitors all mentions of the Office across most social media channels and blogs. In this way, they would be alerted to the fake account almost immediately, and depending on which platform it was created on, they would alert the web 2.0 service to have it removed. If this is not possible, we will continue to monitor the account and issue a statement on the Office's website and social media channels to alert people about it.
Legal: risks that cause legal action against the Office	**Legal liability:** A citizen holds the Office liable for damaging consequences of information provided via an Office web 2.0 service. This may include when the Office publishes third party content (re-tweeting a news article) or when a third party publishes content about a stakeholder on an Office social media platform.	Major	Unlikely	All: Facebook, Twitter, YouTube, Vimeo	Any advice provided on the Office's social media channels will be cleared by subject matter experts before publishing. All planned content will be available in the social media calendar and accessible by Managers to review. A disclaimer about third party content that may appear on the Office's social media platforms is visible in the Office's social media guidelines. There is also a disclaimer about this on Facebook and Twitter. This details that third party views are not endorsed or agreed to by the Office.