STRATEGY AND IMPLEMENTATION
This report presents case studies and examples from international best practice, showcasing positive, successful social media strategies and their implementation. The United States has invested significant resources into the area, including further funding in 2012 for cyberinitiatives, including social media communication, marketing and engagement. In contrast, the defence forces of the United Kingdom, Canada and New Zealand have opted to take a slower and more cautious approach to social media. While the size of the United States’ population could be one reason for its greater engagement in the social media space, another is its desire to be at the forefront of all military technologies.

The core values of a society and the laws governing the rights of its citizens necessarily inform its outlook on social media. The United States has a constitution that explicitly enshrines many personal freedoms, whereas the other countries reviewed here (as well as Australia) have less formally defined personal rights. The United States feels that it has obligations to give and encourage access to instruments that promote free speech, including social media.

Despite the heavy emphasis in this report on policies and practices from the United States (and the US military’s domination of offshore best practice examples), US strategies are tailored to meet challenges and demands that differ from those facing the Australian armed forces. Before embarking on any social media planning, strategy or policy development, Defence as an organisation should ask and answer the simple question, ‘Why should Defence and its brands use social media?’

It is clear from Australians’ high use of social media that those channels cannot and should not be ignored. However, why Australia would follow the lead of the United States when the goals and values of our military forces are different is not so clear. Much can be learned from the US forces’ implementation of procedures and their production and management of content strategy and policy documentation, but for Australia to do what is best for its citizens and military personnel Defence must evaluate the importance of social media and the organisational goals that they can help to achieve. After that, Defence will be able to ‘cherrypick’ from international experience to fashion an approach ideally suited to Australia.
It is easy for social media advocates within Defence to become envious of the resources available to the US armed forces for general cyber and specific social media initiatives, but comparisons should consider the unique objectives and values of each country. Using the United States’ social media standards, values and initiatives as a basis for comparison, the questions set out in Table 4.1 can help to clarify the goals of Defence and how they can be achieved using social media.

<table>
<thead>
<tr>
<th>What?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the organisational or campaign goal and key performance indicators?</td>
<td></td>
</tr>
<tr>
<td>What other channels are being used to achieve the goal?</td>
<td></td>
</tr>
<tr>
<td>What is the budget or resource allocation for the campaign?</td>
<td></td>
</tr>
<tr>
<td>What are the Defence’s legal (public and employee) obligations in this space?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Who is trying to achieve the goal?</td>
<td></td>
</tr>
<tr>
<td>Who is the audience for the campaign?</td>
<td></td>
</tr>
<tr>
<td>Who should engage with the public on behalf of Defence?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Why?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Why is this goal important?</td>
<td></td>
</tr>
<tr>
<td>Why is social media the right channel for the campaign?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>When?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>When should the goal be achieved?</td>
<td></td>
</tr>
<tr>
<td>When will the campaign/communication begin and end?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Where?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Where is the goal? (A country? Online?)</td>
<td></td>
</tr>
<tr>
<td>Where will the social media strategy be implemented?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>How will the goal be achieved?</td>
<td></td>
</tr>
<tr>
<td>How will the strategy be implemented?</td>
<td></td>
</tr>
<tr>
<td>How will it be monitored?</td>
<td></td>
</tr>
<tr>
<td>How does Defence keep up with technology and cultural progress without spending significant resources on continually learning new technologies?</td>
<td></td>
</tr>
<tr>
<td>How can individuals interested in military topics be grouped and marketed to efficiently?</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.1: Clarifying goals for social media
This review shows that there are pockets of highly effective social media practice and guidelines in the Services. However, it has been acknowledged at all levels that a centralised approach to social media strategy, policy and governance is required. Defence’s work not only in the social media, but also in the overall digital space, lacks clear strategy, policy and governance.

Therefore, Defence should consider establishing the proposed Digital Executive Oversight Committee (DEOC), headed by a senior social media adviser. DEOC would provide executive sponsorship and guidance to ensure that the Services’ strategies and tactics are aligned with broader Defence business objectives. The committee should have balanced representation from across the Services and include the Ministerial and Executive Coordination and Communications Division and CIO Group, Personnel Strategies and Policy Group, Defence Community Organisation and Intelligence and Security Group. DEOC should ensure that social media practice is strategically linked with the overall mission and objectives of Defence. Even though strategy and direction would be centralised, resourcing should remain locally based, in order to address the unique needs of the individual Services and ensure responsiveness.

A centralised and coordinated understanding of how Defence, and specifically the Services, will use social media is crucial to ensure successful and appropriate use of the channels. That understanding will affect the development of policy and the use of social media for professional and personal purposes by Defence personnel. A coordinated approach to the high-level components will be extremely important to ensure that the Navy, Army and Air Force and the Department of Defence can each use social media appropriately as they see fit. While each of the Services has a wide variety of requirements and its use of the channels will vary, its activities should ultimately align with the core strategic principles set out centrally.

Any attempt by Defence to coordinate all social media centrally runs the risk of creating approval bottlenecks, which could reduce the speed and authenticity of the conversation and engagement. Organising social media requires a hybrid approach to management: top-down leadership should influence medium- and long-term strategy and policy, but day-to-day management should be decentralised.

DEOC should set out high-level guidance defining unofficial and official use of social media. The committee should also define the depth of Defence’s social media policy as it relates to both professional and personal use, be it on base, off base, within the Defence Restricted Network, in Defence housing, or when deployed. DEOC members will be required to invest considerable attention over the short term. However, once the channel strategies, policies and operational controls have been finalised, the committee should only be required to meet 4–6 times a year to monitor performance and understand the changing landscape.

The proposed structure would also support centralised expenditure for incremental resources such as monitoring and moderation. In addition, the committee would support visible executive sponsorship of social media in Defence.
4.1.1 Strategy management

The suggested strategy governs the overall social media approach by Defence and aims to involve senior personnel in communications strategies. Each of the Services has already set out its organisational goals and values, so this process is designed to ensure that social media and digital technologies are governed by robust policies that support them. The process diagrams in Figure 4.1 and Figure 4.2 are intended to provoke discussion. Each stage will need to be clearly defined and controlled by Defence to ensure stakeholder acceptance.

Figure 4.1: Strategy management process
4.1.2 Campaign strategy

The suggested campaigns or initiatives follow the same process, without the option of adjusting policy, with the expectation that clear metrics will be available to measure the results of each campaign. This process involves stakeholder engagement with subject matter experts to produce engaging content that meets the goals of the organisation and the campaign (Figure 4.2).

Figure 4.2: Campaign strategy process
4.1.3 Goals and objectives

The ‘crawl, walk, run, fly’ concept is often used in business to describe the growth and launch process, either of the organisation or of a particular strategy within the organisation. Those stages can be applied to Defence’s social media marketing and engagement goals. The first three steps (crawl, walk and run) are applied to all organisational and campaign initiatives, while the final step (fly) is the implementation of a crisis plan when the need is identified (for details, see Figure 4.3 and Table 4.2).

A communications crisis plan must be a part of the overall communications strategy. Planning and education should be designed to give responsibility to those who need it in order to communicate in the space with the required speed and efficiency. The crisis plan, or ‘flying’, cannot continue indefinitely and is only used to manage specific sets of predefined issues.

<table>
<thead>
<tr>
<th>CRAWL</th>
<th>WALK</th>
<th>RUN</th>
<th>FLY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BUILD FRAMEWORK</strong></td>
<td><strong>IMPLEMENT FRAMEWORK</strong></td>
<td><strong>EXPAND FRAMEWORK</strong></td>
<td><strong>ENGAGE CRISIS PLAN</strong></td>
</tr>
<tr>
<td>• Engage stakeholders</td>
<td>• Organisational structure (roles and responsibilities)</td>
<td>• Review monitoring and identify issues</td>
<td>• Identify crisis</td>
</tr>
<tr>
<td>• Form executive committee</td>
<td>• Formalize policy and content strategy</td>
<td>• Document successes and failures</td>
<td>• Plan response</td>
</tr>
<tr>
<td>• Establish goals, KPI’s and metrics</td>
<td>• Implement training program</td>
<td>• KPI’s reviewed</td>
<td>• Respond to crisis</td>
</tr>
<tr>
<td>• Develop draft policy and content strategy</td>
<td>• Implement monitoring software</td>
<td>• Integrate offline and online strategy</td>
<td>• Monitor response</td>
</tr>
</tbody>
</table>

Based on the findings of this review, the various Defence social media initiatives range from crawling to taking their first tentative steps. These initiatives have an established framework of social media sites with teams in place to deliver content and engage visitors. While they are in need of some organisational refinement as documented in this report, that work is currently underway.
Table 4.3 shows Defence mission statements and how they might be translated into goals for social media.

<table>
<thead>
<tr>
<th>Mission statement</th>
<th>Social media goals</th>
</tr>
</thead>
</table>
| **Australian Army.** The Australian Army’s mission is to provide a potent, versatile and modern Army to promote the security of Australia and to protect its people and interests. | • Communicate message/image of a potent, versatile and modern army.  
• Increase and engage potential recruits and create a dialogue that may lead them to join.  
• Engage friends and families of personnel to maintain Defence community welfare. |
| **Royal Australian Air Force** The Royal Australian Air Force (RAAF) provides air and space power for Australia’s security. It is the youngest of the three armed Services in the Australian Defence Force (ADF) but the second-oldest air force in the world. | • Communicate message/image of the RAAF.  
• Increase and engage potential recruits and create a dialogue that may lead them to join.  
• Engage friends and families of personnel to maintain Defence community welfare. |
| **Royal Australian Navy** The Navy’s role is to promote and protect Australia’s interests at sea using a mix of ships, submarines and aircraft manned by highly trained and skilled personnel and equipped with appropriate sensors and weapons systems. | • Communicate message/image of protection, highly trained personnel and superior equipment.  
• Increase and engage potential recruits and create a dialogue that may lead them to join.  
• Engage friends and families of personnel to maintain Defence community welfare. |
| **Defence Jobs.** The Defence Jobs website provides detailed information on all Navy, Army and Air Force careers. You can search for jobs, access online services or register for My H.Q. — a secure web site where you can make an online application. | • Increase and engage potential recruits and create a dialogue that may lead them to join.  
• Maintain an engaged audience for broadcast communications and campaigns. |
| **Defence recruitment centre – overseas applicants.** Defence is looking for serving or ex-serving foreign military personnel, who can directly transfer their job and life skills to whatever Service they join. If you are not an Australian Citizen or Permanent Resident, you may still be eligible for entry into the Australian Navy, Army or Air Force. | • Seek out former foreign military personnel and engage them in dialogue about Defence.  
• Harness the skills of trained, experienced service members. |
### Table 4.3: Defence/ADF mission statements – social media goal comparisons


<table>
<thead>
<tr>
<th>Mission statement</th>
<th>Social media goals</th>
</tr>
</thead>
</table>
| **Defence Reserves Support** The Defence Reserves Support provides a link between the Australian Defence Force (ADF), employers and the community from which Reservists are drawn. This site provides information for both reservists and their employers. It includes information about the Reserves and recruiting information for those wishing to join. | • Increase and engage potential recruits and create a dialogue that may lead them to join Defence.  
• Maintain an engaged audience for broadcast communications and campaigns. |
| **Defence Signals Directorate** The Defence Signals Directorate is Australia’s national authority for signals intelligence and information security. | This subject is likely not to be suitable for social media.                        |
| **Directorate of Oceanography and Meteorology** The website of the Royal Australian Navy’s Hydrographic Meteorological and Oceanographic Group, which provides maritime geospatial information and services to meet Defence requirements and national obligations. METOC consists of four sections: Operational METOC Centre; Nowra Weather and Oceanography Centre; Ocean Data Services; and METOC Geospatial Services. | • Educate stakeholders about the services provided by the directorate.  
• Provide a contact and content point for potential media research.  
• Promote the work of the directorate through positive, popular and unique content, such as photos. |
| **Global operations - Australian Defence Force** The global operations page for the Australian Government Department of Defence provides information relating to global operations that Australian Defence Force personnel are currently involved in. | • Provide information to media and communities about global operations. |
| **Royal Australian Air Force Multimedia Site** The Royal Australian Air Force multimedia site includes video clips, video downloads, podcasts, games, images, childrens resources, interactives and kids media. | • Communicate message/image of the RAAF.  
• Increase engagement with existing content through sharing. |
4.1.5 Moderation

A balance needs to be struck between allowing individuals to express their opinions and protecting the community from offensive behaviour or postings. Moderation is the manual or automatic process for assessing and possibly removing such material. Clear guidelines should be posted to the channel where communication occurs, so that contributors are aware of their obligations. Software is available to automate moderation for basic breaches, such as the use of profanities. However, human behaviour in social media is best monitored by other humans, rather than by software.

Moderation is not the removal of opinions or ideas that contradict an official line, which would be considered censorship in the social media. It is the removal of material considered to be extreme and offensive by the majority of the contributing community. What is acceptable in one community may not be acceptable in another. Boundaries are defined by a combination of the community members, the site administrator, the brand and the mechanics or site used for the interaction.

The following material is generally moderated from commercial or government websites or social media channels:

- profanities (at an age-appropriate level for the audience)
- abuse and personal attacks
- hate and discrimination
- obscenity
- personally identifying information.

Additional information that should be moderated for Defence includes:

- security breaches
- breaches of the general code of conduct
- incorrect information.
4.1.6 Monitoring

Monitoring has four primary purposes:

- to identify content that is considered a security breach or requires moderation
- to gather statistics in order to measure the success of a campaign or piece of content
- early identification of potential crises
- brand and subject trend identification and analysis.

In order to moderate significant volumes of conversation, Defence should develop a monitoring process that uses a combination of social media monitoring software and human analysis. The process will depend on the overall goals of Defence’s social media strategy and the individual KPIs of each of the commands and owners of social media presences. The owners should be responsible for their own monitoring and moderation, but too much latitude would create inconsistencies in data collection and make it difficult to compare initiatives accurately. The monitoring process should be standardised across all of the Services to allow direct comparisons and analyses, and conducted at either senior level or by coordinators under the direction of the senior social media adviser.
4.1.7 Branding

Branding is a proactive process that starts with the ‘Plan’ phase (Figure 4.4).

![Figure 4.4: Branding – proactive process](image)

4.1.8 Crisis management

Crisis management is a reactive process that starts with the identification of the crisis (Figure 4.5).

![Figure 4.5: Crisis management – a reactive process](image)
4.1.9 Channel strategy

Defence currently uses social media only in what it considers to be ‘safe spaces’. Those spaces are usually online networks frequented by families and are by nature supportive. Each of the Services is having some success in social media, but they lack clearly defined goals, consistent reporting methods and internal promotion of achievements, causing their efforts to go mostly unnoticed. When considering a channel, it is important to consider how the channel can be monitored, moderated and analysed to ensure that it is meeting defined KPIs.

A social media channel strategy should not be developed as a stand-alone plan. The choice of channel must take into consideration both the channel’s ability to achieve a goal on its own and its ability to complement and support other digital or traditional media channels. It is logical to select a social network with the most members in the target demographic. Currently, for Defence, that would most likely be Facebook, but individual communications may be better suited to other channels such as blogs, forums or Twitter, depending on the goal of the communication.

Questions to ask before selecting a channel include the following:

• Does my goal require two-way communication and audience participation? Why?
• Can the message be communicated using short form text (microblogging)?
• Which other channels are being used to achieve the goals?
• What content (and content types) will be published for the campaign/communication?
4.2 BRANDING STRATEGY

4.2.1 Brand health

The review team used BrandAsset Valuator (BAV) to better understand the current ‘health’ of the Defence brands.

BAV is Young & Rubicam’s proprietary research tool, and is the largest database of consumer opinions in the world and a rich source of brand intelligence in Australia.

An annual Australian online survey of 1,000+ questions undertaken by 2,500+ consumers provides access to:

- 25 million brand facts
- information for 1,200+ consumer brands in 110+ categories
- 58 exclusive brand metrics
- 17 years of continuous tracking to date
- annual data refreshment and category definition for subscribing clients.

Data from BAV, shown in Figure 4.6 and Figure 4.7, demonstrates that a wave of negativity in popular media about Defence issues is out of step with the sentiments of the general public. Each of the Services ranks in the top 6th percentile of all brands in BAV, making the Defence category second only to the Australian Emergency Services category (ambulance, fire brigade, police and SES).

The Navy, Army and Air Force are some of the most liked, even loved, brands in Australia, and all three have gained in all aspects since the 2009 BAV survey (Table 4.4).

In the future, this type of information should be sourced, tracked and where appropriate communicated internally to Defence members. Many members consume journalistic content and accept that it reflects the opinion of the community in general. Qualitative and quantitative research shows that this can cause a misplaced belief that Defence is losing the support of the public. This review suggests that such a notion should be challenged.

To date, BAV has not included government departments in its research, so similar reporting was not available for the Department of Defence. The department is to be included in 2011 research yet to be undertaken.
Table 4.4: BrandAsset scores for Navy, Army and Air Force

<table>
<thead>
<tr>
<th></th>
<th>BrandAsset score</th>
<th>Overall position in 2010 BAV brandscape (1,061 brands)</th>
<th>Esteem score in 2010 BAV brandscape (1,061 brands)</th>
<th>Esteem position in 2010 BAV brandscape (1,061 brands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navy</td>
<td>94.61</td>
<td>58</td>
<td>98.58</td>
<td>16</td>
</tr>
<tr>
<td>Army</td>
<td>98.20</td>
<td>20</td>
<td>99.62</td>
<td>4</td>
</tr>
<tr>
<td>Air Force</td>
<td>98.01</td>
<td>22</td>
<td>99.72</td>
<td>5</td>
</tr>
</tbody>
</table>

*BrandAsset score is an overall rating that combines levels of brand strength and stature. It indicates overall performance of the brand ranked against all brands in the BAV brandscape.*
4.2.2 Employer brand

Many public sector organisations and businesses struggle to establish meaningful brand values because their employees see their brand as the domain of marketing and sales departments. For some, brand is reduced to a clever line or a logo. Defence suffers from no such problem, as brand values are at the core of the organisation. The brands’ inherent values are taught from the point of induction and are the mainstay of education and delivery throughout an individual’s journey through Defence. ADFA cadets refer to brand values as if they have known them from birth.

Brands are, by their nature and through the consistent delivery of experiences, a short cut to underlying values. Over time, people come to understand the experience they should expect from any given brand.

Defence has a clear set of brand values:

- **Professionalism, Loyalty, Integrity, Courage, Innovation, Teamwork**

In turn, each of the Services has a set of values specific to its own culture and needs:

- **Navy** – *Honour, Honesty, Courage, Integrity and Loyalty*
- **Army** – *Courage, Initiative and Teamwork*
- **Air Force** – *(from vision)* *One team – Swift, Decisive, Resilient and Respected*

The representation of the brand values in official social media is essential to ensure that the brand remains consistent. Social media guidelines for Defence members should also refer to the values; while some will be more pertinent than others, all should be considered as part of the process.

There are no better brand advocates and ambassadors than an organisation’s committed members. This is a branding truth that has already been recognised for some time throughout Defence and during campaign development, well before the advent of social media. Throughout social media engagement, the ‘power’ of Defence people is enabling Defence brands to deliver, in the words of one member, ‘our story, our way’, to great effect.

Using members as brand ambassadors has the added advantage of helping to create a desirable employer brand. This form of branding should aim to attract and inspire potential recruits and their parents and friends. Nevertheless, the employer brand is delivered through actions and behaviour, not through endorsed communications in official channels, which should be left to the PR and communications teams.

While the review team was given the task if defining a brand strategy to enable the enhancement of Defence’s brands in social media, the brand direction of ‘people first’ currently being used is the ideal method for engaging in social media. The review recommends that the pursuit of this underlying principle continue unchanged.
One noteworthy challenge of this branding method is that, if members are placed at the centre of a communications strategy, any negative action by any members of the group will inevitably reflect more strongly on the brand – a reality that could be said to be true for Defence in recent months. The challenge can be compounded by one of the main social media phenomena affecting society (businesses, governments and Defence alike): the blurring between the personal and the professional identities of individuals and the organisations they may represent. The personal identity of a user is now published online in an easily sharable format, and younger people view privacy as a value differently from the generations who preceded them. This increase in online content sharing means that the personal qualities, habits and activities of an individual can reflect on their employer, sometimes generating a negative brand image.

4.2.3 Channel ownership

The desire of individuals to sculpt their identities in social media drives many to connect with and promote subjects that interest them and help to define their identity in their networks. This structuring of identity can sometimes lead to individuals creating pages or profiles for organisations they participate with, often without support or approval from the organisation. It can be said that if an organisation does not create its own official channel, someone else may create an unofficial one. The unofficial channel may generate engagement with the organisation’s audience that does not complement and may even conflict with the official message in other channels.

The idea that some control over content and message is better than no control at all inspires many organisations to reluctantly create presences in social media.

It can be argued that if an unofficial page is building engagement with an audience, the audience wanted to engage with that brand in the first place. The real owner of the brand may miss a valuable opportunity to connect. Unofficial presences, particularly in areas with controversial messages and strong ‘for’ and ‘against’ audiences, can be damaging to the reputation of the organisation’s brand.

The Navy, Army and Air Force publicise their official channels on their official websites. However, research revealed dozens of associated sub-brand Facebook pages for Defence. It is unclear whether those pages are official, unofficial, official/unofficial or unofficial/official – all terms used by Defence staff to describe them. The volume of sub-brand sites is likely to result in an inconsistent brand experience being communicated to the community.
This labelling issue demonstrates a level of confusion among Service members. In addition to other reasons, Defence members have indicated that they started Facebook pages and other social media presences to bypass what is described as a slow and heavily governed process for publishing content to the official Defence websites. It is also true that the official websites attract different audiences and therefore social media offers extended communication reach. However, if social media become the channels of choice for Defence communicators, it is possible that an increasingly poor experience will be delivered to the users of the official websites.

It is important to note that the identity of Defence as a brand is not on the whole a social identity. With the exception of some specific events, the organisation does not usually promote social activities to outside communities; nor does it have a requirement to encourage day-to-day engagement with the general public about its activities. The goals of Defence are, in many ways, contradictory to the traditions of social media, where openness and transparency are often considered more important than security and confidentiality. Defence should see social media as tools to achieve many goals, not as an obligation to create a ‘social defence force’ at the potential cost of security.

4.2.4 Brand assets

A positive and consistent brand representation can benefit the organisation not only through creating a sense of trust in the sites and content being viewed, but also by establishing consistency across sites covering different subjects that are clearly identifiable within a single brand family.

In traditional media, communications and marketing teams are usually responsible for the brand imagery of an organisation – a consistent look and feel using mechanics such as language, logos, graphics, colours and images.

A potential brand control would be to provide a resources section for relevant Defence staff on official websites, or intranets with logos and pre-designed social media graphics (such as Facebook skyscraper profile banners). This content would be displayed with clear instructions for its use and details of its copyright restraints. Potentially, the inclusion of ‘social media ready’ logos on the Department of Defence’s Australian Defence Image Library website would satisfy this requirement; however, this review has not investigated the governance of the site.

Defence may wish to develop a process by which members and the general public can report potential copyright infringement and unauthorised uses of brand image mechanics in social media. Defence could then consider reporting infringements to the channel owners or administrators and asking for the offending materials to be removed.
4.2.5 Recruitment branding

Social media provide an obvious way to engage potential recruits with content that represents the values of the individual Services or Defence as a whole.

Understandably, many potential recruits are drawn towards the three Service brands and attempt to engage with the Services and their members in the social media environment. The demographic profile of social media users, the platform and in many cases the content being delivered contribute greatly to recruitment. Then again, due to the organisational structure and in some cases the beliefs of Defence and Defence Force Recruiting, many potential recruits are being redirected to Defence Force Recruiting’s own website or phone number. This is understandable and is intended to ensure that the potential recruit receives the best advice possible. However, from a brand perspective it can seem slightly dismissive, and not only for the individual – the redirection is often posted publicly and is visible to the wider online community.

A number of activities that engage potential recruits via official Defence social media sites have been conducted. While those activities are covered elsewhere in this document, it is worth noting that the engagement was highly effective and produced many ‘likes’ for the pages. In social media, ‘likes’ are a brand currency for future communication.

4.2.6 ‘Test and learn’

Defence should implement an internal process for documenting and promoting the outcomes of social media activities to its social media stakeholders. This would counter negativity towards the use of social media, but also improve on the ‘test and learn’ culture. For many organisations, test and learn methodology can deliver meaningful insights into the use of social media for their brands. If there is no proper documentation of achievements (and failures), the real benefits of such factors as effort and cost reduction are not easily realised.

4.2.7 Department of Defence – a different brand?

Governments and their departments regularly receive negative comments about policy development and service management. This is partly due to competition between social groups.

The Department of Defence as a government body should consider its approach to official social media differently from the individual brands of the Navy, Army and Air Force. For example, department staff may want to engage members of the Defence community and the public in open forums to discuss issues such as the development of policy. With that type of engagement in mind, Defence should consider the resources required, the ability of the community to use the online environment to voice alternative opinions, and whether such a strategy supports the overall goals of Defence. It may well be that the current practice of using the department’s official website (rather than social media) best suits its role and needs.
The branding needs of the Department of Defence will ultimately require a much larger consideration of overall Australian Government needs and directions, and so have been considered out of scope for this review.

4.2.8 Point of failure – reliance on individuals

Defence employees in communications roles are driven to monitor social media manually, in their own time. Their commitment is likely to be unnoticed, despite the significant value it provides to the organisational brands. One concern of the review team is that this creates ‘single points of failure’—when a person leaves a position, an entire communications channel is left unattended, with a detrimental effect on the brand.

This voluntary service has also created an expectation of service after hours. Contributors expect responses to posts within minutes or hours, not days or weeks as existing approval processes require. Defence will need to define its commitment to this ‘always on’ aspect of social media. The commitment is currently defined by the need to moderate content, not the need to engage with users.

4.2.9 Content strategy

In social media, content is at the core of all activity. Discussions, promotions, photos, articles, links and so on are all content, without which social media would simply be called ‘chat’ or ‘communication’. The act of sharing creates the ‘social’, and content (or information) creates the ‘media’.

Content is the tool with which the unengaged can be reached via the engaged. That is, those who are already engaging with the content can attract those who are not by sharing the content in their own networks. The engaged (Tier 1) audience is likely to be very interested in the content or subject, and in the case of Defence is likely to comprise staff, family members and other stakeholders. The unengaged (Tier 2) audience comprises their friends and networks who may have some interest in the content or subject once they have seen it.

A social media content strategy can drive interest in offline communications, such as phone or general digital communications (for example, a website). However, even if it is a stand-alone strategy it should still consider other marketing objectives outside social media and ensure that it is complementary – not contradictory.

Ideally, the general content plan would be set by an executive committee and the senior social media or digital adviser in consultation with the communications team for each Service. This ensures that vertical pillars and horizontal topics complement each other, providing a connection between the Services that is not currently seen in social media. For example, the subject of hospitality and catering is relevant for all the Services, and content produced in that area can be used across the vertical pillars (Figure 4.8). In particular, if the Services are looking to recruit chefs, marketing across the three Services to promote that career would not only Defence Force Recruitment to achieve its goals, but would give each of them the opportunity to showcase their own work in that area.
Content can be themed daily, in the style of the US Army’s five-day content plan, or through weekly, monthly and annual plans that take into account diarised Service events and give the marketing and communications teams clear guidelines on what is expected of them. Weekly meetings with a social media adviser and the coordinators from each of the Services are opportunities to exchange ideas, identify positive and negative conversations, improve processes and identify potential crises.

The content shown in Figure 4.9 showcases 20 Navy chefs gaining work experience at the ARIA restaurant in Sydney. Matching this type of content with a recruitment drive for hospitality staff would not only help to achieve the recruitment goal, but would be likely to increase morale within Defence hospitality services.

Exciting roles, such as operating guns and planes, are often promoted through content, while seemingly less exciting roles such as cooking food for the troops are given limited exposure and promotion. There are good stories in every area of Defence, and they can be used as content to achieve specific goals and targets for recruitment and other purposes.
4.3 POLICY STRATEGY FRAMEWORK

Once a clear strategic direction for social media has been established for Defence by the executive leadership, policy and governance should be established to reflect the new way forward. Defence (as well as the individual Services) has already begun to develop the necessary policies, guidelines and SOPs. The work of the social media teams can be further enhanced through the establishment of the DEOC, which will be able to review all of the existing documentation to ensure consistency and alignment.

By ensuring that its social media policies are clear and concise, Defence can minimise confusion and ultimately establish confidence and clarity for all Defence personnel. The primary Defence policy addressing elements of social media (DI(G) ADMIN 08-1), requires updating to address the complexity of the social media space. This review’s best practice and legal obligations audits demonstrate the need to have a social media policy either as a subsection within DI(G) ADMIN 08-1, or as a separate policy.

The objective of the new policy is to set bounds for Defence members’ use of social media, whether as part of a member’s professional responsibilities or in a personal capacity, to limit the risk of damage being caused to the organisation and members by that use. As Stephen von Muenster said in Section 2.2 of this report:

“A properly drafted and enforced Defence social media policy is Defence’s most effective risk management tool in protecting the organisation from reputational damage and legal liability from the use of social media in during both professional use and private use.

With clear parameters for appropriate conduct during professional and private uses of social media, personnel can ensure that their online behaviour does not put them in breach of Defence’s Values, Code of Conduct or DI(G) ADMIN 08-1.

4.3.1 Policy components

Defence should consider the following policy components, which address the complexity of the social media landscape.

Scope of policy

The policy should focus mainly on the human behaviour associated with communicating online or via social media. It should be platform-flexible, as new social media platforms are being launched at a rapid rate. Should Defence limit itself by defining rules by platform, such as Facebook or Twitter, the organisation runs the risk of policies becoming outdated relatively quickly. It is important to ensure that the policy is able to respond to changes in the social media landscape, such as the recent release of Google+. The policy should be updated as required so that it remains relevant, and members need to be made aware of any changes. Additional training may be required as the policy evolves.
Defining channels and use

There is an opportunity to properly define social media policy with reference to three types of channel and their corresponding uses (Figure 4.10).

![Diagram of social media channels]

**Organisational communication** occurs within official Defence social media channels, which are channels established and run by Defence, such as the Australian Army Facebook page. Any use of them by Defence personnel constitutes organisational communication. These channels should all be listed in the Defence social media registry, and they should be actively monitored and moderated by Defence social media personnel.

**Professional communication** occurs within unofficial channels, but implies affiliation with Defence. These are channels established by individuals or organisations with a vested interest in Australian defence activities, such as Defence veterans or community support groups. Use of these channels by Defence personnel constitutes professional communication and imposes greater responsibility on personnel to represent Defence appropriately.

**Personal communication** occurs within the remaining social media channels (private channels). This includes social media channels with no affiliation with Defence. Use of these channels by Defence personnel constitutes personal communication. Defence members should neither claim nor imply that they are speaking on behalf of Defence when using private channels. If a member discloses that they are a member of Defence, they must state that their views are their own and not those of Defence.

Although these three types of social media channel and three types of use are the focus of Defence’s social media policy, they will never be mutually exclusive. Therefore, the areas where the channels and uses intersect need to be addressed.
Overarching Defence policies and values

To provide context for Defence’s social media policies, Defence should inform personnel about rules and regulations that would supersede the Defence social media policy embedded in DI(G) ADMIN 08-1. It should remind members to familiarise themselves with their terms of employment and all other applicable Defence policies and instructions, including those covering the escalation of issues and the consequences of policy breaches. These include:

- Legislation
  - Archives Act, 1983
  - Defence Force Discipline Act 1982, section 58
  - Public Service Act 1999, section 13
  - Privacy Act 1988, section 6

- Regulation
  - APS Values and Code of Conduct in practice, Australian Public Service Commission
  - Defence security manual, Part 1 – Protective security and Part 2 – Internet content

- Policy
  - DI(G) ADMIN 10-6 Use of Defence telephone and computer resources
  - DI(G) PERS 35-3 Management and reporting of unacceptable behaviour

- Guidelines
  - OPSEC and force preservation awareness training
  - Living the Service values
  - DIMPI 2/2003 – Hand-held imagery metadata standard and procedures.

Defence should consider reviewing its level of tolerance for personal use of social media by members during work hours, whether using a personal device or a Defence-owned asset. As a minimum, access to the official Defence sites should be considered. This review has noted that certain technical restrictions on the Defence Restricted Network, such as bandwidth, also affect access to social media sites; that also needs to be taken into consideration.
4.3.2 Policy for personnel who manage ‘official’ social media

As part of its policy review, Defence should consider personnel who are responsible for the administration and management of official social media sites. They potentially require specific policy considerations in addition to the Defence Restricted Network and the computer assets they need to perform their jobs efficiently.

Authorisation protocols for allowing public comment will need to be reviewed so that administrators of social media are able to respond to posts in good time, mitigating the risks associated with failing to post prompt responses. The protocols should be closely aligned with the social media crisis response procedures.

Defence should also consider reviewing policy to ensure that those tasked with professional communication via social media are considered within policy such as DI(G) ADMIN 106.

4.3.3 Social media engagement principles

Social media engagement principles should establish expectations that are not explicitly covered in existing policy, and also demonstrate how existing policy may be interpreted in the social media space. Defence may develop social media policy covering the three categories of social media channels and uses outlined in Section 4.3.1. For the purposes of policy development, professional and personal use may be considered together, recognising that Defence personnel can never fully separate their behaviour in social media from the Defence brand.

The following points, which are informed by the legal obligations audit, should be considered when developing social media policy.

**Organisational use of social media**

- Only those authorised to comment may do so as representatives of Defence.
- Explain the authorisation process.
- Set out what can and cannot be done, for example:
  - Disclose that you are an employee/contractor of Defence, and use only your own identity or an approved official account or avatar.
  - Disclose and comment only on information classified as public domain information.
  - Ensure that all content published is accurate and not misleading and complies with all relevant Defence policies.
  - Ensure that you are not the first to make an announcement (unless specifically given permission to do so).
  - Comment only on your area of expertise and authority.
  - Ensure that comments are respectful of the community in which you are interacting online.
- Adhere to the terms of use of the social media platform or site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.

- If you are authorised to comment as a Defence representative, you must not:
  - post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a court suppression order, or is otherwise unlawful
  - use or disclose any confidential or secure information
  - make any comment or post any material that might otherwise cause damage to the reputation of Defence or bring it into disrepute.

- Set out a moderation policy and approval processes.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications.

**Professional and private use of social media**

- Have a separate set of guidelines (best practice).
- Do not restrict use, but encourage best practice behaviour.
- Provide a frequently asked questions section.
- Provide examples of acceptable and unacceptable social media communications. For example, state that members must:
  - take responsibility for what they post
  - disclose and discuss only publicly available information
  - ensure that all content published is accurate and not misleading and complies with all relevant Defence policies
  - expressly state on all postings identifying them as Defence members that the stated views are their own and are not those of Defence or the government
  - provide the suggested disclaimer (‘The views expressed are mine alone and do not necessarily reflect the views of Defence.’)
  - be polite and respectful to all people they interact with
  - adhere to the terms of use of the social media platform or site, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws, and other Defence policies and guidelines.
• State that members must not, for example:
  ▪ post material that is offensive, obscene, defamatory, threatening, 
    harassing, bullying, discriminatory, hateful, racist, sexist, infringes 
    copyright, constitutes a contempt of court, breaches a court 
    suppression order, or is otherwise unlawful
  ▪ imply that they are authorised to speak as representatives of Defence 
    or the government, or give the impression that the views they express 
    are those of Defence or the government
  ▪ use their Defence email address or any Defence or government logos 
    or insignia
  ▪ use the identity or likeness of another member or contractor of Defence 
  ▪ use or disclose any confidential information or personal information of 
    others obtained in their capacity as Defence members
  ▪ make any comment or post any material that might otherwise cause 
    damage to the reputation of Defence or bring it into disrepute.

• Set out what is reasonable and unreasonable private use and give examples.
• Refer to privacy, confidentiality and information security in accordance with 
  existing Defence policies and guidelines.
• Address copyright and defamation issues.
• Include a reference to all related Defence policies and guidelines.

Finally, the policy should provide guidelines for escalating cases of the inappropriate 
use of social media. Personnel, and especially commanding officers and warrant 
officers, should have the necessary understanding and tools to address issues related 
to the social media space. Specific briefings for commanding officers on social media 
engagement for both professional and personal use will be required.

4.3.4 Policy development and implementation

Defence may consider developing and implementing social media policy as outlined 
above, using the following outline of work:

1. Define the role of social media in Defence.
2. Review and rework current key policy pertaining to social media.
3. Align other related policy.
4. Review and rework Service-specific policy.
5. Communicate the finalised policy to members through a program of education.

To implement the new policy effectively, Defence must focus on providing appropriate 
educational and training materials to deal with the diversity of attitudes and behaviours 
towards social media within Defence. Education is critical to change management and 
the successful adoption of social media in line with Defence policies and values.
4.3.5 Role of social media in Defence

Before embarking on policy review and revision, Defence should clearly define what social media is (and what it is not) in the Defence context, including what constitute social media content, channels and use. Defence should also articulate the role of social media in Defence, and define organisational, professional and personal use of social media. The high-level policy must be platform-flexible, have executive sponsorship, and be culturally appropriate in the Australian governmental and legal context.

4.3.6 Current policy on social media

While this review identified a number of social media guideline documents, it identified only one official policy that spans all Defence services and organisations: DI(G) ADMIN 08-1 Public comment and dissemination of official information by Defence personnel, which was issued on 5 October 2007 and last reviewed on 5 October 2010.

While DI(G) ADMIN 08-1 makes some inroads in governing social media practice in Defence, there are opportunities for clarification. First, while social media are considered within the document as part of ‘new media’, it lacks a clear definition of ‘social media’. There are also some internal inconsistencies in it that may result in misinterpretation and confusion.

Defence should consider reviewing the DI(G) ADMIN 08-1 policy and creating a new section that outlines how existing policy should be applied in social media contexts. It is important that existing policy covering public comment and official information dissemination is not contradicted by the social media policy.

Once social media has been defined and policy inconsistencies have been resolved, Defence may wish to develop a decision tree type guide to help personnel locate the social media policy section appropriate to their situation (an example is shown in Figure 4.11). A platform-neutral scenario tree will help provide high-level guidance to personnel, without having to have guidelines for every situation that might arise.
4.3.7 Alignment with other policies

It is important that other references to social media in documents such as the Protective security policy are complementary and do not make any conflicting statements.

Another specific policy for review is the DI(G) ADMIN 10-6 Use of Defence telephone and computer resources. Because of rapid technological advances, DI(G) ADMIN 106 requires a clearer definition of computer use and personal devices (such as smartphones and PDAs). It should also address the needs of social media teams within Defence who require access to social media sites to conduct Defence business, such as Facebook page administration.

Service-specific policies and organisational policies for organisations such as ADFA should be reviewed and revised. The overarching policy should set the social media direction for all of Defence, and local policy should stipulate how that is executed locally to accommodate unique needs. Again, local policy should be consistent with and not contradict central social media policy, including SOPs.

4.3.8 Standard operating procedures for personnel

SOPs for administrators managing official social media channels

Both the Navy and the Army have already drafted some guidelines and SOPs for administrators of social media channels. That material should be reviewed to ensure that it is consistent with the overall social media policy. Although the Services have slightly different requirements, they should collaborate to ensure broad consistency in guidelines, policies and endorsements by senior command.
Terms of use for official channels

The terms of use should be consistent for all official Defence social media channels. DEOC should review the current terms as published on the individual Service pages and advise on updates as required.

SOPs for Defence personnel who use social media

By clearly defining and communicating acceptable and unacceptable behaviour in social media use, Defence will mitigate its risks. Past problems involving social platforms may have been exacerbated by unclear definitions of appropriate and acceptable behaviour.

The language and tone of the SOPs for all Defence personnel should include everyday and vernacular terms, as in international best practice documents examined in this review and as used in the US Army social media handbook. Official needs and OPSEC should be demonstrated through examples and should be conveyed in clear, everyday language.

Defence may wish to reserve the right to ask that certain subjects be avoided and to request members to withdraw certain posts or remove inappropriate comments resulting from private use when the interests of Defence and a member's employment are involved.

Australian Defence Force Academy

ADFA should also consider reviewing its social media rules and educational practices to comply with the broader Defence social media policy. Although there might be some slight differences due to the position of cadets within Defence, establishing proper social media behaviours early will minimise potential career risks at a later date. Given the average age of the recruits and their likely level of internet use and integration into social media activity, it is important to ensure that they understand their obligations and responsibility to behave in an appropriate manner.

4.3.9 Education

Education is fundamental in establishing baseline for social media use across Defence and for effective implementation of the policy. To date, social media education has been sporadic, and has relied on the exercise of ‘common sense’ and ‘professional judgement’. While the organisation may have its own clearly defined view of what it requires, the exercise of discretion requires the subjective interpretation of these terms by individuals, some of whom are relatively young, inexperienced and unable to foresee the damage that may be caused by the inappropriate use of social media. Therefore, Defence should consider reviewing all its social media training packages to align them with the updated policy. The training materials should demonstrate how the central and local policies interlink and should also emphasise the overarching ‘ground rules’, such as OPSEC and Defence values.
While central social media education should focus on guidelines and principles, locally delivered education should focus on scenarios that personnel in the particular Service might find themselves in because of their local circumstances. For example, an Army cadet may be more vulnerable to social media misuse at home, while a deployed seaman may be more likely to compromise Defence when blogging to family back home. Local education should also address ‘common sense’ explicitly, to alert personnel to assumptions they might have made based on their own experiences.

Education and training need to be tailored to different stakeholder groups, according to their requirements and level of understanding of social media:

- Executive-level training should focus on education about opportunities and risks associated with social media use and should ‘on board’ leaders in the organisation.
- Middle managers should be equipped with the skills and knowledge to support and help implement social media practices within their local areas. This can include details such as approval processes for content publishing on the official social media channels and escalation procedures for inappropriate use.
- Personnel should be trained in how to use social media to ensure the responsible representation of Defence, and in how to access relevant policy.

Finally, education should go beyond Defence personnel to include families’ social media activities. Family and friends should be provided with support and guidelines to communicate safely with their loved ones using the channels. The guidelines can also be provided to the Defence Community Organisation, Defence Family Matters magazine and Defence Families Australia to reinforce the necessity to protect family privacy, OPSEC and security.
4.4 CRISIS MANAGEMENT STRATEGY

To mitigate communication risks in social media effectively, it is necessary for Defence to define clearly what type of content is concerning or undesirable. Various content could cause concern, but Defence should be able to set out a scale for prioritising responses that balances the severity and the probability of particular types of postings. Once a scale is available, escalation procedures can be carried out to respond in a timely and accurate manner. To be considered a crisis, the communication of undesirable information will be very rapid, very wide, or both.

Not all undesirable content will produce crises, so a triage system for assessing problem content as it comes to hand should be implemented. This will ensure that problems are mitigated appropriately, according to the probability that they will produce a crisis and the severity of resulting damage. The aim is to prevent crises occurring by identifying and dealing with problems early, where possible. Should a crisis escalate, Defence should be prepared to address it according to the crisis management protocol.

PR teams are best equipped to generate reactive communication to protect the brands and reputation of Defence. However, negative mentions in traditional media do not necessarily drive negative social media conversation. Often, negative mentions can encourage positive conversations, as advocates in social media defend the brand against the traditional media’s positioning of the issue. Before responding to negative sentiment or postings, it is necessary to identify the type of problem as well as its severity.

Social media crises can include the following types:

- OPSEC breaches
- personal security or privacy breaches
- Marketing/PR – originated offline – propagated online
- Marketing/PR – originated online – propagated online
- Marketing/PR – originated online – propagated offline.

Identifying the source and type of breach helps to define the most appropriate response. While this review was given the task of examining the management of employee-generated crises, problems in social media can originate from a variety of other sources,
such as the media, online communities and the general public.

The management of a crisis that originates in social media but is propagated offline (usually by mainstream media) should follow Defence’s existing procedures for media management, with the addition of maintaining a vigil in the social space. However, Defence’s ‘offline’ procedures are mostly understood by a few public affairs specialists, so high-level documentation would be beneficial in defining online processes. The remaining types of social media crisis should be handled online. Suggested actions to be taken in response to a social media crisis are set out in Table 4.5.

<table>
<thead>
<tr>
<th>Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSEC Breach &gt; online</td>
<td>• Remove offending content (or request its removal).</td>
</tr>
<tr>
<td></td>
<td>• Contact individual responsible for breach and educate them about their actions in the first instance.</td>
</tr>
<tr>
<td></td>
<td>• If the individual continues the breach, disciplinary action should be taken in accordance with Defence disciplinary protocol.</td>
</tr>
<tr>
<td></td>
<td>• Monitor for rumours or rebroadcasting of material and, where possible, replace rumours with facts.</td>
</tr>
<tr>
<td>Marketing/PR offline &gt; online</td>
<td>• Respond to all channels with a consistent message</td>
</tr>
<tr>
<td></td>
<td>• Monitor for rumours or rebroadcasting of materials and where possible replace rumours with facts.</td>
</tr>
<tr>
<td>Marketing/PR online &gt; online</td>
<td>• Respond online only (no need to deepen or spread the crisis)</td>
</tr>
<tr>
<td></td>
<td>• Monitor for rumours or rebroadcasting of materials and where possible replace rumours with facts.</td>
</tr>
<tr>
<td>Marketing/PR online &gt; offline</td>
<td>• Apply existing offline crisis management processes.</td>
</tr>
</tbody>
</table>

Facebook provides crisis management guidelines for commercial businesses using social media. Some of the guidelines, such as identifying the problem and determining the validity of the source, clearly apply to Defence (Figure 4.12). Other points, such as ‘Empower your loyal consumers and advocates’ can apply to family members in Defence’s ‘safe spaces’ in social media. Defence community members should not be expected to shield Defence or its brands, but some will inevitably attempt to do so, motivated by loyalty and pride. This is another reason why Defence should consider a wider education program for social media use that goes beyond its own personnel.
Crisis management, PR, marketing and branding are all interconnected, which implies that a crisis plan cannot be developed without the involvement of stakeholders from all of those fields, in addition to Intelligence services. The ‘crawl, walk, run and fly’ business strategy, as outlined in Section 4.1 of this report, works as a strategy for Defence in social media. The ‘fly’ phase is actioned only when a crisis is occurring and should be developed as an important part of the overall strategy. Crisis management is generally reactive, but can be developed proactively with a marketing and communications plan to provide communications staff with guidelines on how to react.

The key steps in the crisis management plan are to identify the crisis, plan the response in line with the guidelines, respond to the crisis, and monitor the response (Figure 4.55). Those steps continue until a crisis is no longer identified in Phase 1. Crises or potential crises can often be identified through regular monitoring and careful moderating of social media spaces using a combination of software and human analysis.
4.4.1 Crisis identification

The following questions should be asked to assess whether a negative situation might be considered a crisis and how a response should be developed:

- What is the type of issue?
- Is the issue in more than one channel?
- Can the issue be managed through existing offline crisis management methods?
- Will a response aggravate or mitigate the crisis?
- Are there legal considerations to the response?
- Who is the best person to address the crisis?
- Are offline media likely to quote responses or escalate the situation via traditional channels?

Communications staff responsible for managing social media should be given the training to respond to negative situations quickly and flexibly. Social media are a few of many channels where communication occurs, and many journalists use them to investigate or source stories. Therefore, public relations in the social media should be given the same consideration as broadcast media public relations.

Not all Defence members need to use social media to communicate officially with the general public, just as they are not all permitted to talk officially to the traditional media. Official communication should be restricted to those who are experienced at communicating the message of Defence in other channels, but with specific crisis management training in social media and other digital channels. Approval processes for communication in a crisis should be fast-tracked so that core values are upheld, without delays in responses that could create a knowledge void (described below) and further damage to Defence.

4.4.2 Tips for communications staff in responding to a social media crisis

- Stay in your lane (respond only to issues within your area of expertise or that you have consulted knowledge owners about).
- Consult a social media adviser before taking action.
- Take a breath. Fill space carefully, not emotionally.
- Consider whether your response will inflame the crisis or create a new one.
- Delete and/or report OPSEC breaches immediately, and inform the social media adviser and the individual responsible for the breach.

While communications staff should receive special training and resources to respond to social media crises, other personnel will also require guidance on reporting and escalating concerning content they see in social media channels.
4.4.3 Emergency response monitoring

In addition to day-to-day monitoring, emergency monitoring can be set up in a crisis. It can include a combination of feeds and alerts designed to give an instant snapshot of conversations happening online. Standard monitoring tools often take 24 hours to process data, which can be too slow in a crisis. Emergency monitoring should bring together a combination of near realtime tools and continuous human monitoring of all conversations for the duration of the crisis. Responses to that information can then be made instantly or fed to the communications team for further advice.

4.4.4 The ‘knowledge void’

A knowledge void is an inactive period during communication that creates an opportunity for rumours to start and unofficial presences to expand and grow. For example, when a negative comment is posted about Defence, the lag time between the initial comment and a response from Defence creates a knowledge void.

To counter this possibility, Defence should aim to be the trusted source of information for the audience. Consistent branding is one way audiences identify information as ‘official’, which is why it is important for the Services to have a well-managed and well-populated presence in social media before a crisis arises. This ensures that community members will know where to get factual information directly from the source, allowing them to share it with their networks and thereby aid the crisis management effort. In addition, if a response must be delayed, the issue should at least be acknowledged and the expected response time provided in order to manage expectations.

This review discusses crisis management in Defence-owned social media channels, but ignoring content in unofficial channels can also produce a crisis. If no official information is available, unofficial channels have an opportunity to communicate their own ‘information’ or agenda, which can then be shared by others in their networks. This action can have the opposite effect of crisis management and can create a new crisis through the spreading of rumours or untruths, often unintentionally. Communities want information about issues that affect them, and gaps in knowledge will often be filled by someone with a receptive audience ready to believe unofficial and potentially incorrect information.

If you don’t become the trusted source for information, someone else will.
4.4.5 Crisis exit strategy

In early trials of social media within Defence, several pages were created that were later abandoned due to lack of results or resources. It is important that these and similar future pages are not simply left in cyberspace without any information about why they are no longer active, while at the same time acting as an alternative source of information. For example, this review found a locked Defence Twitter account with no explanation about why the account was locked. This creates the impression that Defence is publishing material that it does not want open to the public. While that is not true, the effect on the brand could be negative and the action could generate rumours and false information.

Most such trials are conducted in ‘safe spaces’, and there is nothing wrong with informing the audience that a social media presence is a trial or in beta. It is often beneficial to engage the audience in the trial and make them feel part of the process by allowing them to provide feedback. This has the added advantage that questioning users about their experience in order to improve the site does not raise suspicions. It also means that problems with the page can be raised with the audience, which usually produces positive support from users.

If the goal of the social media presence has not been met or a lack of resources makes it impossible to continue, that should be communicated to the audience. This can be done by publishing a post stating why the page or presence is no longer active, with a link or direction on where to go for further information or to contact the owners. In the case of Facebook, skyscraper profile pictures can be used to communicate the movement or closing down of the page. However, once the message is communicated, a dead space should not be left in social media.