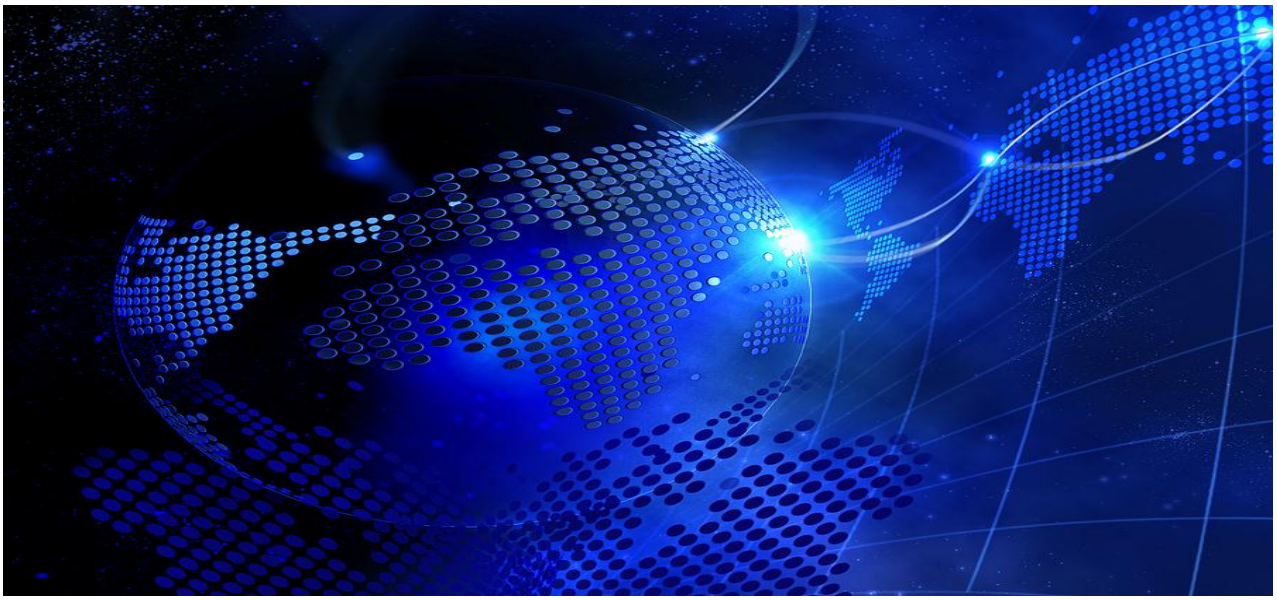
NITA UGANDA

- Driving the IT Revolution -



GOVERNMENT OF UGANDA SOCIAL MEDIA GUIDE

Version Number:	1.1
Date:	July 2013

DOCUMENT DETAILS

Security Classification	Government/Public		
Authority	National Information Technology Authority-Uganda (NITA-U)		
Author	National Information Technology Authority-Uganda (NITA-U)		
Documentation Status	**Working Draft** √	**Consultation Release** ☐	**Final Version** ☐

CONTACT FOR ENQUIRIES AND PROPOSED CHANGES

All enquiries regarding this document should be directed to the Office of the Executive Director.

info@nita.go.ug

ACKNOWLEDGEMENT

This version of the guidelines on Social Media for the Government of Uganda was developed by the Department of Architecture, Standards and Certification under the Directorate of Planning Research and Development, National Information Technology Authority-Uganda (NITA-U).

Feedback was received from both internal and external stakeholders to NITA-U which was greatly appreciated.

Foreword

Social media is a set of online technologies, sites and practices which are used to share opinions, experiences and perspectives. Fundamentally it is about conversation.

Social media in this context is a dialogue that happens between Government and its citizens. This means that the level of control assumed from traditional media is replaced with a deeper level of engagement with the public. The main benefit of social media for governments is that well-considered and carefully implemented social media can create greater transparency, an interactive relationship with the public, a stronger sense of ownership of government policy and services, and thus a greater public trust in government.

The potential uses of social media are wide and varied. Government can use social media to raise awareness of certain issues, build credibility with specific audience groups, engage the public on policy consultation, or as an internal communications tool to improve collaboration between government agencies or within a single agency.

Due to the significant rise and uptake of social media tools in Uganda, it has become necessary to consider Social media in developing any modern, professional communications strategies especially within Government operational domains.

Social media is useful as part of the broader efforts to engage with citizens. In addition to facilitating citizen communication and consultation on policy initiatives, social media can be used to support recruitment, as well as for awareness and sensitization initiatives.

It is imperative to choose the most appropriate social media tool. Simply picking and using a Social Media site because it is popular can be counterproductive if it is not suitable for the intended purpose. Planning to use social media should be done as part of a wider effort to determine an agency's engagement strategy. Once an agency understands its engagement strategy, it can then determine which social media tools will best meet its needs.

It is in light of the above, that the NITA-U has developed these guidelines to guide Government Ministries, Departments and Agencies in the process of adopting Social Media as one of the Platforms for engaging with the citizens of Uganda.

The NITA-U shall within its mandate continue to provide technical guidance in the implementation of these guidelines as well as the rollout of Social Media in a manner that facilitates it secure adopting and development across Government MDAs.

Thank you

Executive Director

List of Acronym

CEO : Chief Executive Officers

IT : Information Technology

NITA-U: National Information Technology Authority-Uganda

MDA : Government Ministries, Departments and Agencies

MOICT: Ministry of Information and Communications Technology

RSS : Rich Site Summary

Definitions

Social Media: Social media is a set of online technologies, sites and practices which are used to share opinions, experiences and perspectives. In contrast with traditional media, the nature of social media is to be highly interactive.

Executive Summary

This document has been written to aid Government MDAs in the proper choice and usage of Social Media to suit their specific needs. It establishes basic principles, addresses code of conduct and legal and security issues related to the use of Social Media in Government MDAs.

As with any communications channel, social media require proper planning, benefit and risk assessment, resourcing and commitment. The requirements to be considered in the rollout of Social Media across MDAs have also been stipulated.

Finally a business case template designed to stimulate thinking around some of the key areas that need to be considered when planning to use social media has also been provided.

Table of Contents

1. Introduction

The Government of Uganda recognizes the importance of Information and Communications Technology (IT) in economic development and has initiated major steps to promote its use. One of the major initiatives is to improve IT infrastructure so as to bridge the digital divide and lower the cost of communication.

The government is leveling the ground through formulation and implementation of policies and regulations aimed at attracting investments in the sector. There has been tremendous growth in the number of Institutions providing Internet services, suppliers of computers and related accessories/equipment which have stimulated the introduction IT Services such as Social Media where users can interact and share information in real time in a variety of formats such as text, video, pictures and audio among others.

Cabinet in May 2013 directed the Ministry of Information and Communications Technology (MoICT) to ensure that every Government Ministry, Department and Agencies (MDAs) opens a Twitter and Facebook account to improve communication with the Public.

The Government of Uganda is committed to the principles of Open Government, which means transparency in process and information participation by citizens in the governing process public collaboration in finding solutions to problems, and participation in the improved well-being of the citizens.

Accordingly, the Government is committed to engaging effectively with its citizens in a meaningful, accountable, responsive and equitable way.

In light of the above, NITA-U within its mandate embarked on the development of these guidelines to facilitate secure usage of Social Media (Facebook and Twitter etc.) for efficient exchange of Information across Government Ministries, Departments and Agencies (MDAs) as well as improving effectiveness of communication, sharing of information and open engagement and discussions with the Public.

1.2 Purpose

These guidelines have been developed to assist Government MDA with the management of social media use across Government MDAs domains. The document contains guidelines for using social media. It is envisaged that the Government of Uganda will increasingly use social media to interact with citizens or the public to encourage openness and promote transparency and efficiency in Service delivery to the Citizens through secure platforms.

These guidelines provide a secure framework for online participation by the Government MDA to share and information and responses to the Public for good Governance.

The Guidelines stipulated therein apply to all Government employees within the respective MDAs who use social media for official purposes. They are intended to cover future social networking services as they develop. These guidelines will be regularly reviewed to reflect changes or advancement in technology.

1.3 Audience

This document is intended for Government MDAs using or in the process of adopting social media as an official communication channel. It also provides general guidance for using social media tools and as well as the use of Government IT infrastructure to access social media for personal use.

2. Basic Requirement for use of Social Media

2.1 Resource Planning

Resource planning for social media is especially important.

1. Social Media requires both the hardware and Software platform which must be planned for well at the initial stages of implementation. The hardware platform provides the communication interfaces where users can interact, post and view text, pictures and video etc.

2. It is in addition important for MDAs to have dedicated bandwidth for users to upload and download content inform of text, video, pictures and video etc. Agencies need to budget for this as they do for other infrastructure needs. A genuine assessment of the likely costs (with a real understanding of the benefits) should be undertaken.

3. MDAs shall dedicate resources required to create back-ups, transcripts, and other records of social media activity.

4. Forums that debate specific policies, however, may be time-specific. Resource planning should take that into account.

5. It takes time to build an on-line community, therefore resource commitments need to reflect scalability.

2.2 People

2.2.1 Self-Learning

1. The best ways for Government staff to learn how to use social media is to start off using it themselves by encouraging them to setting up their own personal Facebook or Twitter profile or starting up a personal blog in their own time. This will help them to learn with minimal risks, and

without the added weight that comes with representing the agency in a professional manner. Once staffs have learned they will be better prepared to start using social media professionally.

2. Staff should only engage in social media on behalf of the Agency if they have received the authority and where necessarily trained to do so.

2.2.2 Trusting staff

Social media tools require quick responses and direct communication with stakeholders, often in real or near-real time. It is important to note that:

1. Successful social media activities are ones where delegated staff (appointed based on Government Standing Orders and the Communication Policy of Government or the Institution) is trusted, after proper training, to understand and manage the risks around release of information. If information needs further verification or is potentially contentious, staffs need to be trusted to escalate as appropriate and those escalation paths must be quick and efficient.

2. Nothing kills the effectiveness of a social media involvement more quickly than slow response times where each and every statement or 'tweet' needs to go up the chain of command to be approved before publication.

2.2.3 Accounting Officers and Chief Executives

The Heads of Institution in the respective Government MDAs should put into consideration the following prior to adoption of the use of Social Media as communication Channel within their organizations:

1. When undertaking any new communications strategy, all channels should be considered, and if social media is deemed appropriate, Heads of Institution need to consider the risks, benefits, goals, and audiences before directly participating. An Accounting Officer's presence on social media should be considered part of the larger communications strategy.

2. While social media has benefits, it needs to be actively managed if the benefits are to be realised and the risks minimised. One of the most serious drawbacks is the amount of time social media takes up and the risk that, if they are not familiar with social media. Consideration should be given to resourcing or delegating to a social media expert within the Government MDA.

3. As with any media tool, Accounting Officers or Chief Executives should ensure they are adequately trained in using social media before they begin participating. It is a public forum, and should be considered as such at all times. Content posted in error in social media often cannot be withdrawn and may damage the Government MDA reputation, as well as the professional reputation of the Accounting Officers.

2.3 Content Management

1. Government MDAs shall ensure that information or content to be posted are verified and approved by the relevant Authority.

2. Ensure that the content to be posted or published through social Media is intended for the right audience and is in line with the topic being discussed which relate to the Agency

3. Ensure that the materials to be posted on a Social Media site is not fraudulent, harassing, threatening, bullying, embarrassing, sexually explicit, profane, obscene, racist, intimidating, defamatory or otherwise inappropriate or unlawful.

4. Ensure that posted material on Social Media site is representative, accurate and contains collective views of the Agency (single understanding voice by all in the Agency).

2.4 Considerations for use of Social Media

Before embarking on the use of social media in Public service, Government MDAs shall consider the following:

1. **Entity Goals and objectives:** It is important to consider the goals and objectives of the entity and specifically what the entity would wish to communicate and accomplish by the use of Social Media as a communication channel across the different MDAs as well as with the Citizen.

2. **Entity target audience(s):** Government entities should conduct analysis and prioritization of its audience to achieve the purpose for communication through the use of Social Media. This is important different audience(s) require different information as well as feedback or response. Therefore Social networking may be fashionable but it is not the best communications channel in every instance or for every audience

3. **Benefits, risks and mitigations for those risks**: It is important to clearly understand the benefits Social Media contribute to the entity as well as the risk associated with its use in Public domain including the putting in place mitigation measures for these risks.

4. **On-going resources required:** Government entities shall dedicate resources both human and IT infrastructure for the success implementation and rollout of Social Media in Government MDAs. MDAs should continuously invest in human resource development to handle responses, feedback and the responsibility of ensuring that only appropriate content is released to the Public.

5. **Measure for success:** Using social media successfully requires successful relationship management. Successful relationship management requires a consistent approach in the way in which a Government entity conducts itself through its social media account (how fast an entity responds or provide feedback, how often the entity's Social media site is updated, how often the entity conducts statistical analysis of its followers on the Social media sites and the number of responses provided etc.)

3. Guidelines for use of Social Media in Government MDAs

Social media is useful as part of the broader efforts to engage with citizens. In addition to facilitating citizen communication and consultation on policy initiatives, social media can be used to support recruitment, as well as for awareness and sensitization initiatives.

It is very important to choose the most appropriate social media tool. Simply picking and using a website because it is popular can be counterproductive if it is not suitable for the intended purpose. Planning to use social media should be done as part of a wider effort to determine an agency's engagement strategy. Once an agency understands its engagement strategy, it can then determine which social media tools will best meet its needs.

3.1 Guiding Principles for Official use of Social Media

Government MDAs wishing to use social media as an official communication tool need to familiarize with the following key principles for its use across all forms of social media.

1. Government MDAs shall ensure Credibility in the information relayed through Social media to the public or across agencies by being accurate, fair, thorough, and transparent. Ensure that what you publish is consistent with relevant policies, standards and behaviors.

2. Government MDAs shall ensure consistency and only encourage constructive criticism and deliberations. Employees within the respective Government entities are encouraged to be cordial, honest and professional at all times.

3. Government MDAs shall ensure responsiveness by providing feedback in a timely manner and likewise sharing insights where appropriate.

4. Government MDAs shall whenever possible integrate and align online participation with other offline communications.

5. Government employees are public servants. It is important for them to remember that they are ambassador for their respective agencies. Therefore whenever possible they are encouraged to disclose their position as a representative of the Ministry, Department or Agency as this creates trust among the entities and with the public.

6. Government employees managing their respective entity social media shall be good custodians of information and shall ensure that content and messages are checked and posted regularly. Also ensure that information is created, kept and, if necessary, disposed of in accordance with organisational policies.

7. Government MDAs shall ensure that their employees desist from unacceptable behaviour such as harassment, bullying, illegal or otherwise inappropriate activity whether the Social Media is used as official or private social media account.

8. Government MDAs shall establish protocols in relation to who is authorised to respond to media inquiries or political enquiries received via social media. Timeliness in response may mean additional employees may require permission to reply to enquiries via social media beyond normal approval channels.

9. Government MDAs shall ensure that internal policies are put in place to bar employees form disclosure of information, making commitments or engaging in activities on behalf of Government online unless authorised to do so.

10. Government MDAs shall ensure that employees do not make comment that they are not authorised to make especially where the comment may be taken as official comment.

11. Government MDAs shall ensure that information posted online are approved by the relevant Authorities within the respective MDA. This could be interpreted as an official statement or commitment to some course of action from the MDA. Permission must be obtained for any information to be posted or for discussion of sensitive matters not already in the public domain.

3.1.1 Mixing Official work and personal lives

Be aware of the following responsibilities when mixing official work and personal lives:

1. It is acceptable to use a personal account to comment on matters unrelated to official work provided it does not interfere with official duties.

2. Using a private account will not excuse you from misconduct proceedings if you are identifiable as a Government employee and are proven to engage in conduct that would otherwise amount to misconduct.

3. Government employees/staff shall not publish personal opinions on official social media accounts.
4. Government employees shall remember that their role within the Public Service creates an association between what they say online and the Government itself.

5. Government MDAs shall ensure that their employees do not list or cross promote personal accounts on Government platforms unless authorised. Be clear that your views are your own, when using your personal account.

3.1.2 On-line Discussion of Government Related topics

Government MDAs shall consider the following guidelines when discussing Government related topics on-line:

1. Individuals authorized to comment on behalf of the Government MDA shall ensure transparency and identify themselves when discussing Government related topics

2. Authorized individuals shall identify themselves as Government employees, when publishing content in an official capacity as part of their work.

3. You can only use an official Government account if you are authorized to do so and it is part of your duties.

4. As an identified Government employee, your comments should be apolitical, impartial and professional.

5. When commenting on Government topics on a personal account be sure to make it clear that your views are your own.

6. Always use your judgment when making private comments, particularly to ensure these comments cannot be misconstrued as official commentary (this is particularly important for senior officials for whom separating their private views from their positions may prove increasingly difficult the higher they are in the hierarchy within the Public Service Structure).

3.1.3 Considerations prior to On-line discussions

Government MDAs shall ensure the following:

1. Uncertain information shall not be published

2. Shall ensure that information is correct before posting and advice shall be sought if in doubt because professional credibility may be inseparably linked to the online comments.

3. That advice shall be sought from appropriate arm of Government for responses to questions that may fall outside the area of expertise.

3.1.4 Use your discretion

1. Never publish information that should not be made public always seek permission to publish content that is not already in the public domain.

2. Unless authorized, avoid discussion of industrial or legal issues, and refer these to the relevant arms of Government areas if asked to comment specifically.

3. Always seek advice if in doubt about whether information can be made public.

3.1.5 Codes of Conduct and online participation

The following Codes of Conduct shall be followed by Government employees involved in the use of Social media as a tool for communication:

1. Staff should participate in the same way as they would with other media or public forums such as speaking at conferences.

2. Seek authorization to participate in social media on behalf of the respective MDA. Do not disclose information, make commitments or engage in activities on behalf of government unless you are authorized to do so.

3. If you are participating in social media on behalf of your agency, disclose your position as a representative of the agency unless there are exceptional circumstances, such as a potential threat to personal security.

4. Never give out personal details like home address and phone numbers.

5. Always remember that participation online results in your comments being permanently available and open to being republished in other media.

6. Stay within the legal framework and be aware that defamation, copyright and privacy laws, among others apply

7. If you are using social media in a personal capacity, you should not identify your employer. Doing so would bring your employer into disrepute.

8. Keep in mind that even social media sites restricted to your 'friends' are in effect public, as you cannot control what friends do with the information.

9. Always make sure that you are clear as to whether you are participating in an official or a personal capacity. Be aware that participating online may attract media interest in you as an individual, so proceed with care regardless of what capacity you are acting in.

10. If you have any doubts, take advice from your manager or legal team or relevant authority with the MDA

11. Ensure that any comment you make on matters of government policy is appropriate to the agency role you hold, and remains politically neutral.

3.2 Personal use of social media in the Government

Personal use of social media is defined as individual or private use, using your own personal social media accounts and where you are not commenting as a authorized officer of the Government.

1. Do not use work email or social media accounts for private blogging or other forms of personal online comment. Your personal account profiles should be linked to a personal email address, for a Facebook or Twitter account.

2. Do not use Government email address to establish a personal social media account.

3. When accessing personal social media accounts via the Government MDA IT systems, do so in a manner that does not interfere with your duties and is not inappropriate or excessive.

3.2.1 Acceptable personal use of Social Media

Acceptable personal use of Social Media shall include:

1. Re-tweeting content from your Department account on your own Twitter account

2. Accessing and posting comments within your Department micro blog service (e.g. SharePoint etc.)

3. Engaging as an individual citizen in community debates which do not cross over into your areas of policy responsibility or matters unrelated to your official duties.

3.2.2 Unacceptable use of Social Media

Unacceptable personal use of Social Media shall include:

1. Using Government resources to access or post any material from a Social Media site that is fraudulent, harassing, threatening, bullying, embarrassing, sexually explicit, profane, obscene, racist, intimidating, defamatory or otherwise inappropriate or unlawful.

2. Using the Government IT resources to provide on the record comments to journalists, politicians and lobby groups other than in the course of your official duties

3. Excessive time using social media that is not related to your work.

4. Levels of Involvement and Risk Associated with Social Media

The use of Social media in the respective Government MDAs should be adopted on a systematic basis. Government MDAs do not have to rush to use Social Media on the first day. MDAs may start with passive involvement and move through to becoming more active and finally fully engaged with the audiences identified.

4.1 Passive involvement

Passive involvement in Social Media requires the Government MDA to simply listen to what is being said about the MDA.

Social media monitoring tools may be used to discover what is being said the MDA. The authorized MDA representative may conduct a twitter search for relevant terms (about the MDA name, or the name of a specific issue relevant to the Agency).

At a minimum, the Government MDA representative should find and assess the social media tools that their target audiences are using. This landscaping can then be used to inform strategic plans, future communications, or budgets for greater participation in social media, if necessary.

4.2 Active involvement

Once the Government MDA has listened for a while and understands the tone and concerns of a social Media community, it may begin becoming more active by posting links to information to help people answer questions they have, or can actively correct an inaccuracy on a Social Media forum.

Ensure that the principles **stipulated in section 3.1** are followed and always identify yourself as a public servant if you are responding on behalf of a Government MDA.

4.3 Fully engaged

Finally the Government MDA becomes fully engaged in using Social Media by:

1. Setting up a group on a social networking site and regularly introduce content for discussion
2. Establishing a Twitter or Facebook profile and begin contributing and actively posting and answering questions.
3. It is important to note that once the MDA has become fully engaged it has the responsibility of being a good custodian. There is need to post materials regularly, moderate comments as appropriate, and check regularly for messages that require a response.

4.4 Risks associated with using social media

Because social media is an evolving area of government engagement, there are risks. These can be cultural, technical or reputational and must be factored into planning. But they should not dissuade you from using

social media. Over time, as experience builds and case studies provide us with precedents, risks will be more easily identified and reduced.

Government MDAs shall consider the following risks associated with the use of Social Media:

1. **Misrepresentation and misinterpretation**: Information and views can be spread very quickly and widely through online media and can easily be subject to misinterpretation and misrepresentation. A post by government employees may be inaccurate or inappropriate, creating legal or reputational risk.

2. Government involvement or activity on some social media site and forums may not be welcome.

3. **Lack of control**: User generated content may be difficult to check for accuracy and comments may unintentionally inflame a situation. Once online material is made public there is little control or influence over how it might be used or modified or integrated.

4. **Resourcing:** Establishing, contributing to and moderating social media sites take expertise, time and resources.

5. **Privacy:** There is no guarantee that privacy can be protected.

6. **Security:** High traffic sites/accounts may pose a greater risk for 'malware' or spyware'. Some sites may be open to manipulation by interest groups or those with malicious intent

7. **Time wasting:** – Employees may use social media in a way that interferes with their duties.

8. **Bandwidth**: Some social media requires higher levels of bandwidth.

9. **Accessibility**: Some sites may be blocked or may not provide content in accessible formats.

The official use of social media has the potential to compromise compliance with legislation, particularly in regard to accessibility, privacy and recordkeeping.

Content contributed by anyone may infringe upon the rights of others in areas such as defamation, intellectual property and fraud.

4.5 Social Media Risk Management

The appropriate management of risks associated with Social Media in **section 4.4** are stipulated in the tables below.

Social Media Risk Management

No.	Risks Associated with Social Media	Management of Risks Associated with Social Media
1.	**Misrepresentation and misinterpretation**	• Government MDAs shall ensure that the Information to be posted on any Social Media Site is verified for accuracy and approved by the relevant authority
2.	**Lack of control**	• Government MDAs shall ensure that users are sensitized and trained on appropriate generation of content prior to uploading onto the Social Media site
3.	**Resourcing**	• Government MDAs shall designate one key resource person (s) with expertise to handle all Social Media activities.
4.	**Privacy**	• Wherever possible, Government MDAs should issue a disclaimer alerting users when they are no longer on a government site and that the site's own privacy policy applies
5.	**Security**	• Government MDAs can implement security measures to mitigate security risks e.g. putting in place Institutional Security policies to counter any possible attack or compromise on MDA information or system.
6.	**Time wasting**	• Time wasting should be addressed as a management issue, not a technology issue. Personal use of Social Media should be separated from office use and specifically when to engage in personal activities.
7.	**Bandwidth**	• MDAs need to budget for bandwidth as they do for other infrastructure needs. Assessment of the likely costs (with a real understanding of the benefits) should be undertaken to provide for actual bandwidth requirement.
8.	**Accessibility**	• MDAs should maintain official copies of materials in accessible formats on their Social Media Sites for ease of reference.
9.	**Government involvement**	• Government MDAs shall ensure that engagement with the citizens on Social Media is transparent as possible and further ensure that engagement are those that stimulate National development.

4.6 Benefit, risk and mitigation

The appropriate mitigations measures for the risks associated with Social Media in section 4.4 are stipulated in benefit, risk and mitigation tables below.

Passive →		Active →		Engaged
Monitor	Signpost or support	Respond	Discuss	Debate

Monitor

Potential activity	Potential objectives	Benefits	Risks	Risk mitigation
• Monitor social networking sites, forums and blogs for discussion on the agency, its proposals or services delivered	• Understand how opinion is forming • Identify gaps in service delivery • Identify service users'/audience's information needs • Understand how stakeholders are related	• Situational awareness • Increase understanding of nature and range of commentary	• Monitoring tools are emerging, and standards of practice have yet to be formed • Debate may be unrepresentative	• Should supplement, not replace, other media monitoring and stakeholder activity

Signpost or support

Potential activity	Potential objectives	Benefits	Risks	Risk mitigation
• Provide links to user-generated or government sites for information, advice or discussion	• Increase discussion on live consultation or current services • Signpost information, advice and services to specific groups of users who indicate particular needs • Reduce level of duplicated information/advice provided from government and user-generated sites	• Promote transparency in government by distributing information more widely and publicising government in more places • Lead the Public directly to online transactional services	• Information or advice provided by linked-to site may be inaccurate or misleading • The link may offer sites a competitive advantage, by increasing the volume of visitor traffic • The debate on linked-to sites may contain inappropriate content • Uncertainty around cost/ benefits	• Where feasible and appropriate, use of standard disclaimers relating to content of external (e.g., non-government) sites • Provide contact for other sites to request links • Monitor content of sites to ensure that they are relevant and appropriate

Respond

Potential activity	Potential objectives	Benefits	Risks	Risk mitigation
• Correct inaccuracy on blog, forum or other Social Media • Answer query raised on social networking site, forum or blog	• Increase audience for information • Increase speed of response to misinformation and requests for information • Build trust of public	• Promote transparency in government by distributing information more widely and publicising government in more places • Achieve accurate media coverage by better distribution of clarifications	• Getting the tone of voice correct (it needs to be tailored to the context, and cannot simply be 'government') • Government intervention in site	• Post rules should be prominent and understood by site users • Corrections should relate to facts only, not opinion • Posts should be short and provide links to where details of policy or

	• Move resource-intensive offline tasks to (existing) online self-help communities		may not be welcomed • Corrections of information may not be believed • A post by government may be inaccurate or inappropriate	evidence can be found • Contact centre scripts should be followed when providing information or advice

Discuss

Potential activity	Potential objectives	Benefits	Risks	Risk mitigation
• Set up a group on social networking site • Start discussion thread • Feed in content to a website, or post content on social media site	• Feedback on services • Increase reach of information • Identify gaps in service delivery or information provision • Facilitate discussion across different organisations, e.g. non-governmental organisations, media, government • Move resource-intensive offline tasks to (existing) online self-help communities.	• Reach specific audiences on specific issues • Benefit from the credibility of non-government channels by providing facts and support in the right manner • Complaints may be made, which is an opportunity to truly engage with stakeholders and gain valuable feedback.	• Open to manipulation by interest groups or those with malicious intent • What is the status of complaints made? How will they relate to standard channels? • Responses may be difficult to analyse due to lack of context or difficult to check for accuracy • Government endorsement may add credibility to inaccurate information posted on site	• Clarify how long discussions will be active • Understand the audience of the host site. what profile they have and why they visit the site • Contingency planning to accommodate large number of responses • Select either a pre-or post-moderation approach and ensure that participants understand • Make objectives of clear and what might change as a result • Ensure terms of use

	• Seek input to solutions from the public to regional or national issues or problems		• May generate large volume of responses • May be unable to manage information in accordance with organisational policies	address the handling of objectionable content and hostile commenters • Clarify how organizational Information Management policies will be applied

Debate

Potential activity	Potential objectives	Benefits	Risks	Risk mitigation
• Set up a group on a social networking site and regularly introduce content for discussion • Instigate an iterative discussion with input from government • Open up material on relevant government site for comment	• Consultation, where appropriate • Move resource-intensive offline tasks to (existing) online self-help communities • Seek input to solutions from the public to regional or national issues	• Benefit from the credibility of non-government channels by providing facts and support in a helpful manner • Complaints may be made, which is an opportunity to truly engage with stakeholders and gain valuable feedback.	• Open to manipulation by interest groups or those with malicious intent • Responses may be difficult to analyse due to lack of contextual information • Could create expectations that results provide a mandate for action • Providing feedback on specific issues needs active management • Heated nature of the debate may prompt participants to say the wrong thing, which is then permanently on	• Communicate objectives to participants • Clarify how long discussions will be active, how information will be used and what feedback will be provided • Identify the level of information about respondents that will be required for analysis • Contingency planning to accommodate large number of responses • Have dedicated resource to actively manage online debate • Establish and communicate clear

			record • May generate large volume of responses • May be unable to manage information in accordance with organisational policies	posting guidelines or rules • Clarify how organisational Information Management policies will be applied

5. Transparency in Using Social Media

Government MDAs should be fully transparent in their interactions within social media, including the addition and removal of content. Any officer responding to and posting new comments should identify the comment as an official response from a Government Agency.

5.1 Identify as an official Government presence

1. When publishing using social media, the different departments within the Government Agency should identify the account as an official Government presence. Personal accounts should not be used when making comment in an official capacity.

2. The other ways to identify and convey the official status of social media presences include:

   (a) Use of Government MDA branding links between Directorate websites and the social media account (for example, link to a page on the Directorate website that also links to the official social media account evidencing its official status)

   (b) Use of customized disclaimer messages or terms of use hosted on the official Directorate website.

5.2 Communicate account closures

Where a Government Agency wishes to close a social media account they should advise via the account both the reasons for closure and options for further communication and engagement with the relevant authorities and the Public.

5.3 Intellectual property infringement

The term 'intellectual property' covers the various legal rights to protect the result of original and creative effort.

Intellectual Property may be infringed by:

1. Re-tweeting or sharing content without acknowledgement by the original author posting photos to a Social Media site without consent from participants.

2. Copying work such as songs, articles, movies, or software, from a source without being authorized to do so is a breach of intellectual property

3. Posting Government content on social media sites whose terms of service do not comply with Government policy.

To avoid intellectual property infringement:

1. Produce content specifically for social media sites.

2. If choosing to post Government content on social media sites, be mindful of the potential conflict between the sites terms of use and the intellectual property requirements

3. Do not post third party information without permission or license

4. Where the third party has provided permission, check the permission whether it is broad enough to cover posting to social media sites.

5.4 Record-keeping

A record can be in written, electronic or any other form, under the control of the Government MDA, kept as a record of its activities, whether it was created or received by the Agency. Attention needs to be given to ensure that information of importance is appropriately captured.

Records created through the use of social media should be captured and managed in accordance with the **National Records and Archives Act 2001.** Determine what records should be kept to document the business function or activity, how long they should be kept, and how they should eventually be disposed of.

It is important to remember that a public record may exist in any format, including emails, text messages and other digital forms.

Common information about the records that may need to be captured includes:

1. Date of discussion or business activity
2. Details of your name and other stakeholders involved
3. Key discussion points
4. Details of instructions or advice provided
5. Approvals, decisions and recommendations made among others

5.5 Accessibility

Where appropriate, content on official social media accounts should be made available in an accessible format to all who need it. The provision of Information should not be discriminatory.

It may also be appropriate to refer individuals to telephone or face to face channels for the access of Information. This creates Public trust in Government.

6. Legal Considerations in the Use of Social Media

The Computer Misuse Act 2011 was enacted to prevent unlawful access and disclosure of information, abuse or misuse of information systems including computers.

Section (26) of the Computer Misuse Act 2011 provides for the prevention of willfully, maliciously and repeatedly using electronic communication to harass or threaten another person with the intention of placing that person in reasonable fear for his or her safety or to that of their immediate family.

This section of the guide therefore provides best practices on how to ensure that use of Social Media does not infringe or defame the rights of individuals or Government MDAs.

6.1 Defamation

Defamation is the injury to another person's reputation either directly or implied through the publication of words or sound. It does not matter if the defamation was unintentional.

Publication of inaccurate information on Social Media Sites that lower public perception of an individual or Government Agency can amount to defamation and should be avoided.

Avoiding defamation by considering the following:

1. Do not post information online that is unsubstantiated relating to a business or individual

2. Avoid re-tweeting or commenting on posts and tweets which may be a rumor or Confidential relating to a business or individual or the Government MDA.

6.2 Negligence

Negligence is the failure to act when bound by a duty of care. Government employees should take reasonable action to avoid acts or omissions which you can reasonably foresee would be likely to injure an individual or the Government entity.

Some of the ways to avoid negligence include:

1. Establish systems and processes to appropriately monitor and respond to social media channels.
2. Avoid providing advice or recommendations unless part of your standard customer service scripting or information passes through official approval processes.

3. Explicitly set expected response times and state any limitations to responding (such as during business hours), or disable comments (where possible) if resources are temporarily unavailable. If such a situation occurs involving a Twitter account, tweet a message to this effect.

4. Recommend appropriate channels for certain types of communication (such as emergencies).

6.3 Privacy and Security

Social media by its nature can result in the disclosure of personal information in a public way. Privacy is one of the major concerns of those using social media and legal advice should be sought in relation to compliance with the relevant information privacy laws in place.

There is no guarantee that social media users' privacy will be protected to a sufficient degree. Wherever possible, agencies should issue a disclaimer alerting users when they are no longer on a government site and that the site's own privacy policy applies.

Openness and transparency should be the defaults, meaning blocking users on a Social Media site designed for public interface is not advisable.

Government MDAs shall consider the following to ensure that privacy and security in use Social Media is maintained.

6.3.1 Guard against identity theft

It should not be assume that anything posted online is completely private or limited to certain groups, or that password protection is enough. Basic information, such as an address, birthday, photo, or mobile number can be combined with other public information, enabling someone to steal your identity.

6.3.2 Respect the privacy of others

It is important to remember that individuals have different comfort levels when it comes to their privacy. Seek permission before posting information, photos or videos, and respect the choices people make.

6.3.3 Stay safe

Caution should be taken not to organize meetings on Social Media. Inappropriate communication (such as threats, harassment etc.) from users shall be reported to the relevant Authorities.

6.3.4 Use the most appropriate method of communication

Communication with a single contact or select group of people may be better done through E-mail rather than using Social Media.

6.3.5 Understand the sites privacy policy

Government MDAs shall consider the strength of assurances given about security of the sites visited and the conditions of acceptance.

6.3.6 Report abuse or misuse

Personnel in the respective Government MDAs charged with the responsibility of acting on behalf the Government entity shall ensure to report abuse or misuse of any Social Media site.

7. Guidelines for Hosting Social Media Sites

While an agency may develop and host an online community, it is the people who join and contribute to that community who make it their own. The community must be genuinely open to citizen-generated content if it is to leverage the power of this medium, and also avoid any reaction from people who feel that they have been marginalized or excluded.

The following are guidelines to assist agencies who have or in the process of creating an online discussion board, blog, social networking page, in order to engage with the community:

1. **Maintain contact with group members.** Many online communities provide the ability to email all members. It is important to use this tool to value-add to the membership; however, it should be used sparingly. Members may not want to be bombarded with emails from government agencies.

2. **Spark conversations.** It is acceptable for an agency to begin a discussion topic to help kick-start ideas for group members to discuss. However, this needs to be planned. The important thing is to avoid saturating it with 'official' topics.

3. **Monitor for inappropriate content.** Contributions that contain offensive, defamatory or other inappropriate content may be removed. Please note this is different from removing negative comments or complaints.

4. **Respond appropriately to negative criticism.** Ownership should be taken of serious negative criticism and not ignored.

5. **Do not censor discussion.** For example, by attempting to remove a comment from a discussion board that is 'negative'.

6. **Avoid saturating with government staff.** The aim of 'official government' social media is to engage with the audience and encourage membership from the general public.

7. **Do not post comments via another user.** For example, asking a member to post a discussion item on the Government's behalf, posing as a genuine comment from the public.

8. **Avoid using the membership list for unrelated marketing purposes.** The members have joined to participate in that group only not to become part of a government mailing list for other, non-relevant information.

7.1 Aligning social media with other channels

1. It is to be expected that official social media accounts will be relied upon as authoritative sources of Government information. Accordingly, it is vital that social media content aligns with that available through other official channels. However, social media platforms may be the first points of publication of Government information in certain circumstances e.g. emergencies.

2. It is preferable that social media is not the primary information source. Instead, social media broadcasts or discussions should be based on, or direct users to, a Government MDA managed point of truth.

3. Government Departmental or Directorate websites or customer service points are the preferred single point of truth and social media posts relating to specific information should reflect or direct users to the best source of truth.

4. Where possible, ensure content exists on directorate websites or customer service points prior to announcing on social media accounts. Avoid using social media channels in isolation to release information to the public or any other stakeholder which has not already been released publicly on a Government website or customer service point.

5. It is important to note that immediacy and 'real time' publication are hallmarks of social media and a communications strategy designed to prioritize social media as a place of first publication may be appropriate in certain situations. Similarly, in emergency events social media users who subscribe to services like Twitter will use official Government feeds as priority information channels (like emergency broadcasts) and they expect constant, immediate updates. In these circumstances, such an account could be used as a live feed of Government information providing timely updates. It would be a mistake to wait for a media release or a media conference before tweeting an evacuation notification, for example.

6. While not every post will necessarily contain a link to verifying content, every account should contain a link to an official Government MDA website in an easily identifiable space e.g. Facebook information section or Twitter bio page.

7.2 Establishing meaningful, manageable social media sites

1. Government MDA should avoid the establishment of social media presences for narrowly defined subject areas such as campaigns instead strategically build a social media footprint with a focus on general customer groups and ongoing relationships. However, in certain cases, e.g. a youth oriented campaign suited to Facebook; such campaign specific sites may be considered.

2. Social media accounts should complement other channels used for major or core activities of the Government MDA and allow business areas to clearly identify which social media accounts are intended to broadly reach the audience sought for engagement.

3. Specific activities are then able to be presented within a broader framework and audience, supporting potentially longer term ongoing relationships based on broader interests that can be transitioned to other activities.

4. The social media presence can be built over time to have an established audience who know and have confidence in that presence, and are readily accessible when new activities are supported via the account.

7.2.1 Committing to ongoing relationships

1. Establishing an official social media account creates an expectation of an ongoing dialogue and engagement with Government. Before establishing social media accounts, Government MDAs should assign appropriate resources in preparation for the continuing relationship expectations of the community.

2. Officers with access to official social media accounts should be appropriately skilled in the use of social media and briefed on their role and responsibilities. Officers should be provided with appropriate training in areas such as social media, media relations, code of conduct, privacy, defamation law and intellectual property.

3. Ideally Officers they should also have the subject matter expertise and delegated authority necessary to represent the Government MDA in that field. The immediacy with which social media content is distributed challenges hierarchical approval methods and it is recommended that social media officers be appointed with delegated authority to represent the Government Agency and supported by appropriate reporting and escalation processes.

4. Officers representing the government MDA through official social media accounts must comply with the Public Service Standard orders or Code of Conduct and should be made aware on how the Code is relevant in an online context.

5. Using social media successfully requires successful relationship management. Successful relationship management requires a consistent approach in the way in which a Government Agency conducts itself through its social media account. This means having an understanding of the Government Agency reputation, always presenting the same persona and using a consistent voice when speaking on behalf of Government.

6. When multiple officers are using the same account, it is advisable that they share an understanding of the Government MDA reputation online and adhere to a common style. Areas operating high traffic accounts could consider humanizing their presence by using official team tweeters.

7.2.2 Managing expectations

When considering the establishment of a social media presence Government MDAs should define the ways in which it will and will not be used.

Consider the following examples of cases when managing expectation:

1. If an account will be used to respond to individuals who contribute messages consider, how will this be managed outside of business hours.

2. What expectation does this raise and how will they be managed.

3. Will you respond to all messages? If not, how does that affect the relationship with others who observe that

4. If an account is not used to respond to individuals, how will this impact upon the credibility of the account, and how can this be managed?

5. Should you simply use an RSS feed for news alerts and information services

6. Be clear with those using the social media presence through both actions and statements.

Consider the following in managing expectations:

1. Be timely and consistent with responses

2. Where individual responses on the social media presence are not made, develop standard responses directing people to other channels such as a phone number, complaints process, contact us page or feedback form etc.

3. Develop standard responses supporting moderation, for example: Posts containing offensive language are deleted as they breach the terms and conditions of this service. View the terms and conditions.'

4. Use account settings that limit the opportunities for contributors to submit offensive materials

5. Develop customized disclaimers or terms and conditions accessible from the social media presence

6. Develop complaints handling procedures for complaints filed via social media. Citizens will likely use these channels as a way of going direct there is need to develop a system to respond, even if that system is simply a referral to online forms.

7.2.3 Responding within social media

Responding to others within social media from an official Government account is an official communication from the Agency, and the choice to respond should be based on deliberate decision making that considers the expectations of users of the service, as well as the risks associated with individual instances and issues.

In addition to considering the risk of responding, Government Agencies should also consider the risks of not responding.

Social media is an interactive channel, and user's initial expectations may be high in terms of responsive access to Government via social media. Whilst through statements and actions these expectations can be mitigated to some degree, the emergence of a significant issue on a social media presence is an opportunity to engage early and directly with those already talking about it to deliver messages that can clarify and defuse.

7.3 Moderating social media

1. Government MDAs have a responsibility to moderate content or messages submitted through social media applications to protect against issues like offensive language and behavior that may breach service terms and conditions.(Note: some social media sites are not able to be moderated, e.g. Twitter, which prevents users posting content to others accounts).

2. Government MDAs have a responsibility to ensure social media is used genuinely, meaning that where users are enabled to publish content or comments they should not be edited where valid criticism or an alternate point of view (e.g. political or ideological) is expressed.

3. Government MDAs should appoint a moderator to review comments either pre or post publication where moderation is possible (it is not possible to pre-moderate Facebook comments, for example).

4. When using social media to seek online comment, Government Agencies should have an acceptable use policy that is clearly displayed on the site that makes it clear that:

    - Contributions should be relevant, non-threatening, respectful of views of others, and avoid insulting, obscene and defamatory comments.

    - Where necessary, the moderator will remove any posts that do not comply with the acceptable use policy.

The moderation process must:

- Be objective and impartial and avoid any perception that posts are being censored for political reasons

- Be sensitive to the diversity of the community and avoid any perception that it is being applied in a discriminatory manner.

- Inform posters why their post has been rejected and give them an opportunity to resubmit.

5. Government Agencies should develop disclaimers accessible via the social media presence that account for social media and advise users on how they manage their social media presence. The disclaimer should be hosted on the official Government Agency website and linked to/from relevant social media accounts.

7.4 Monitoring social media

1. Responding in a timely manner, particularly to critical issues, requires that the Government MDA monitor the activities on its accounts as well as third party social media accounts, tools and websites.

2. While this may seem an overwhelming task, customer research and analytics will help inform the selection of sites, tools and terms that warrant the most attention. It is also recommended that Directorates establish an incident reporting process for the documentation of significant issues and the action taken.

3. As part of a risk managed approach it is advisable that the directorate consider scenarios that may occur through social media and document the response as a guide for official Social Media Officer/s. This will help pre-empt and ensure a consistent response to the community should critical incidents occur.

4. Even if official Government accounts do not exist, monitoring what is said about an issue, Government Agency or topic is an advisable source of information for Government. Monitoring

social media pertains not only to the activities on an official Government account but also third party accounts, networks and groups.

5. Directorates should explore options for moderation management that balance risk and value for money in terms of the activity the social media presence supports.

7.5 Success measures

As with other Government MDA activities, social media accounts should be subjected to measurement to assess whether or not they are achieving business objectives.

Authorized Officers carrying out social media activities on behalf of the Government Agency are responsible for gathering those metrics which have been agreed for their specific channel and providing that data on a regular basis.

Refer to Annex 1: The Business Case Template to provide justification for the use of Social Media as a Communication Channel. The template further provides important considerations for Government MDAs in the process of adopting Social Media as a Communication tool.

Conclusion

This document has been written to aid government agencies in trying to decide if they should use social media in a communications, community engagement or policy consultation context. It is establishes basic principles, addresses code of conduct and legal and security issues related to the use of Social Media as a communications channel. Social media require proper planning, benefit and risk assessment, resourcing and commitment. It is therefore important that the guidelines stipulated in this document are followed together with other relevant Government Policies on the exchange of information over electronic media for the successful rollout of Social Media in Government Ministries and Department.

References

1. ACT Government Social Media Policy Guidelines
   - http://www.cmd.act.gov.au/__data/assets/pdf_file/0020/312581/Social_Media_Guidelines_-_May_2012.pdf
2. SOCIAL MEDIA Guidance for Agencies

   http://files.oper.sa.gov.au/files/socialmedia_guidelines.pdf
3. Guide to Social Media
   - https://marketing.purdue.edu/Toolkit/SocialMedia
4. Social media – How to
   - http://webguide.gov.au/web-2-0/online-consultation/social-media/social-media-how-to/
5. Guidelines and best practices for social media use in Washington state
   - http://www.governor.wa.gov/news/media/guidelines.pdf
6. Social Media in Government - High-level Guidance
   - https://webtoolkit.govt.nz/files/Social-Media-in-Government-High-level-Guidance-final.pdf

ANNEX 1 : BUSINESS CASE TEMPLATE

The template on the following pages can be used to make the outline case for use of social media in a Government MDA.

This document is a guide to setting out the rationale and justification for selecting social media as a communications channel, together with relevant risks and mitigations. As with all other channel evaluation, it is important to consider the context in which it will be applied and how that will contribute towards achieving the overall strategic aims of the Institution.

The suggestions here are not intended to be prescriptive, but instead aim to stimulate thinking around some of the key areas that need to be considered when planning to use social media in any Government Institution.

The following tips should be put into account:

1. **Be specific**: Where possible use hard data to support your business case.
2. **Be realistic**: Identify where there are gaps and detail how they are being addressed.
3. **Be measured**: Build in specific targets and a means of evaluation from the start.
4. **Be integrated**: Consider social media in the context of your wider communications strategy.

No.	SECTION HEADING	PROMPTS FOR INFORMATION IN THIS SECTION
1	**Strategy context and aims**	• What is the context for this social media project? • What are the strategic vision and aim(s) that this work will contribute to?
2	**Communication objectives**	• What are the specific communication objectives that will support delivery of the aims(s), including who you are communicating with and why? • Can these objectives be made SMART (specific, measurable, achievable, realistic and time-bound)?
3	**Critical success factors**	• What does success look like? • What are we hoping to achieve (e.g. changes in attitude, awareness, and behaviour)? • Can success against these factors be measured?

No.	SECTION HEADING	PROMPTS FOR INFORMATION IN THIS SECTION
5	**Audience**	• Who are the audience for this communication? • What information or insight do we have about them (e.g. what are their beliefs, attitudes, behaviours and influences)? • What previous attempts at communication with this audience have been made and what has been learned? • What else is out there in terms of social media for this audience?
6	**Options appraisal**	• Have a wide range of other communication options been considered? What are they? Social media can be one channel amongst others. • Which factors contributed to your selected approach? • What is your proposed approach, what will be the main activities and when will they be implemented? • How well does the proposed approach help achieve the identified critical success factors, objectives and aim(s) of the strategy? • How well does the proposed approach help achieve the identified critical success factors, objectives and aim(s) of the strategy? • How well does the selected approach fit within your wider communications strategy? • Is your chosen approach accessible to your target audience? • Is there any evidence of similar approaches that have been successful, to support the recommended approach? • What trade-offs, if any, need to be made (e.g. foregoing some off the benefits in order to keep costs low or carefully accepting a higher level of risk to achieve more substantial benefits)?

No.	SECTION HEADING	PROMPTS FOR INFORMATION IN THIS SECTION
7	**Benefits**	• What direct benefits can be identified (e.g. return on investment, resource requirements)? • How will direct benefits be calculated? • What indirect benefits are there (e.g. qualities of service, improved credibility, ability to reach specific audiences on specific issues, better understanding of audience views)? • How will indirect benefits be measured? • Are there any trade-offs in terms of benefits (e.g. balancing the level of benefits against risks and costs)?
8	**Risks and mitigation**	• What are the risks or threats to achieving the stated objectives and benefits? • Do you have the necessary skills, experience and resource to support this approach? • Have you ensured that the terms of use and privacy policy of any third party service provider you propose to select are acceptable to your agency, if necessary in consultation with your legal team? • Do you have the relevant authority to do this and have you consulted the necessary communication guidance? • How likely is it that the identified risks will happen and what could the impact be? • What could be done to mitigate the risks and who will own these actions?
9	**Dependencies and assumptions**	• What assumptions underpin this approach and what is being done to test them? • What skills, experience and resource (e.g. IT capability or funding) will be needed to implement this approach? Are they available and, if not, where will they be found? • If the approach does not address all of the communication objectives, what other activity is planned? • How does this approach fit with other strategy and policy issues in the department?

No.	SECTION HEADING	PROMPTS FOR INFORMATION IN THIS SECTION
10	**Resources required**	• What skills, experience and resource will be needed to implement this approach? Are they available and, if not, where can they be found? • How much on-going resource will be needed to maintain this approach and is it available? • Will delivery be largely in-house or will an external provider be required? • What is the total budget required?
11	**Evaluation**	• How will success at all levels (i.e. against benefits, critical success factors and specific objectives) be measured? • Have you considered both quantitative (e.g. number of interactions) as well as qualitative (e.g. measure of influence) means of evaluation? • Are metrics in place to monitor progress against targets/objectives?