DMC-PR-05-07-02 dated 5 August 2009

Version 1.0

ONLINE ENGAGEMENT GUIDELINES

SUMMARY

1.   **Service and MOD civilian personnel are encouraged to talk about what they do, but within certain limits to protect security, reputation and privacy. An increasingly important channel for this engagement, and to keep in touch with family and friends is social media (such as social networking sites, blogs and other internet self-publishing). Personnel may make full use of these but must:**

- **Follow the same high standards of conduct and behaviour online as would be expected elsewhere;**
- **Always maintain personal, information and operational security and be careful about the information they share online;**
- **Get authorisation from their chain of command when appropriate (see para 2 below);**

2.   **Service and MOD civilian personnel do not need to seek clearance when talking online about <u>factual, unclassified, uncontroversial non-operational matters</u>, but should seek authorisation from their chain of command before publishing any wider information relating to their work which:**

- **Relates to operations or deployments;**
- **Offers opinions on wider Defence and Armed Forces activity, or on third parties without their permission; or**
- **Attempts to speak, or could be interpreted as speaking, on behalf of your Service or the MOD; or,**
- **Relates to controversial, sensitive or political matters.**

3.   **If in doubt personnel should always seek advice from their chain of command / line management.**

4.   **Service and MOD civilian personnel are encouraged to operate "sponsored" online presences to help communicate their work, including as part of their official duties, as long as these are authorised in advance, registered with MOD London (CIO and DMC), and support Service or Defence communication objectives. Commanding Officers, supported by Media and Communication staff, are responsible for clearance and oversight and should look for suitable opportunities.**

ONLINE ENGAGEMENT GUIDELINES

INTRODUCTION

1.   Current and emerging internet technologies, such as simple self-publishing, sharing of user-generated content and social networking, are of growing importance to Service and MOD civilian personnel in their personal and professional lives.

2.   Service and MOD civilian personnel are encouraged to talk about what they do within certain limits to protect security, reputation and privacy. Such online presences[1] provide an opportunity for Service and MOD civilian personnel to explain their work. But they also carry risks to individuals, to their Service and to Defence. Service and MOD civilian personnel are already using online presences and Defence information is entering the public domain unofficially. Guidelines are therefore required.

AIM

3.   The aim of this guidance is to enable Service and MOD[2] personnel to make full use of online presences while protecting their own, Service, and Departmental interests, and to enable Commanders and communicators to harness this to communicate Defence.

APPLICABILITY

4.   This guidance applies to all serving Armed Forces personnel, reservists and MOD civilians.

POLICY FRAMEWORK

5.   The Defence Communication Strategy and subsequent Defence Online Engagement Strategy[3] set out the MOD's overarching approach to the use of online presences in communicating defence, which is to:

> "…harness new and emerging technologies, new unofficial online channels, and new unofficial online content in order to communicate and disseminate defence and Service messages and build defence and Service reputation, in a way which minimises the risks to personal, informational and operational security, to Service and MOD reputation, and of litigation." [4]

6.   Use of the internet by Service and MOD personnel is governed by existing rules on conduct and behaviour[5], security[6], the use of official IT[7], and contact with the media and communicating in public[8].

7.   Online presences are broadly divided into "corporate"[9], "sponsored"[10] and "personal"[11]. MOD strategy is to harness all three, using our own people - supported by

---

[1]   An online presence is defined here as any channel by which an individual or group self-publishes information online, for example a website, blog, photo or video channel, bulletin board account, social network profile, wiki or multiplayer game avatar.

[2]   This includes: MOD civilians and staff in Trading Funds, Agencies and NDPBs.

[3]   Defence Online Engagement Strategy, Two-Star Approved Draft, August 2007.

[4]   Defence Online Engagement Strategy, Two-Star Approved Draft, Paragraph 19: 'Strategic Intent'.

[5]   Rules on conduct and behaviour for the Armed Forces are set out in the respective Queen's Regulations for the Royal Navy, Army and Royal Air Force. Rules on conduct for MOD Civilians are set out in The Civil Service Code and in the Policy Rules and Guidance promulgated by DCP.

[6]   JSP 440 "The Defence Manual of Security"

[7]   JSP 740 "MOD IT Acceptable Use Policy"

[8]   DIN 2008DIN03-020, "Contact with the Media and Communicating in Public"

professional advice and official facts and figures - to better communicate our work to the public:

- MOD centre and the single Services (via DMC and other authorised bodies) will continue to operate a small number of "corporate" online presences, to communicate the overarching defence mission and put corporate information in the public domain.

- Commanders, with media and communications staff, are encouraged to foster or identify suitable "sponsored" official presences, using material generated at grass-roots by individuals and units, and published with appropriate clearance and oversight (essentially the same as for contact with the media). Such presences are to be authorised at FLC level or higher, registered centrally with DMC and CIO and follow the guidance at Annex A. Service and MOD civilian personnel who feel able to help explain their work to a wider audience should consider volunteering to operate a "sponsored" presence.

- Service and MOD civilian personnel may operate "personal" online presences without Command or Management authorisation or oversight, but are to follow the guidance on conduct and behaviour set out at Annex B.

8.   Commanders and Line Managers should ensure that their staff are familiar with the guidance at Annex B, and consider whether any of their staff could be sponsored to operate a sponsored presence.

MAINTAINING SECURITY

9.   Protecting personal, operational and information security is a critical enabler to all online engagement. Breaching security or disclosing official information without authorisation can be a serious disciplinary offence that could ultimately lead to dismissal or to civil or military legal proceedings. Commanders and Line Managers should ensure that all their staff are familiar with the security guidance at Annex C on the information they should protect when publishing information online.

ANNEXES
ANNEX A: Sponsored online presences – Approval and operation
                    Appendix I: Guidance for personnel operating sponsored presences
                    Appendix II: MOD comment policy
ANNEX B: Guidance for Service and MOD civilian personnel when online
ANNEX C: Guidance on Maintaining Security online

---

[9]   *"Corporate" online presences are the official websites of MOD and the single Services. These are the formal public faces of those organisations online and are operated by the relevant information and communication staffs.*
[10]   *."Sponsored" (also known as "official" or "affiliated") online presences are those presences operated by individuals or units, designed to engage with the public at a personal and informal level but with the official blessing of their Service or MOD.*
[11]   *"Personal" online presences are those operated by Service or MOD civilian personnel outside their official duties.*

ANNEX A: SPONSORED ONLINE PRESENCES – APPROVAL AND OPERATION

1.   **Introduction**   In essence, a sponsored presence is a means for Service or MOD personnel to engage with the public at a personal and informal level but with the official blessing of their Service or MOD.[12] The following guidelines apply in all cases:[13]

2.   **Minimum Criteria**   Sponsored presences must:

- Be authorised in advance;
- Support Service and/or Defence communication objectives;
- Either be part of an individual's work, or at least not interfere with their work;
- Be overseen by local Command / Line Management and/or by media and communication staff - the level of oversight will vary depending on circumstances and subject matter;
- Be centrally registered with DMC and CIO in London and be referenced from the MOD website.

3.   **Approval**   Procedures for clearance and oversight of sponsored presences are the same as for any other official contact with the media, as set out in 2008DIN03-020. Front Line Commands, with the advice of their Media and Comms staffs, may authorise sponsored presences in respect of single-Service matters, but are to inform DMC London[14].   Material from overseas operations must be cleared by the relevant theatre Press Information Centre and by PJHQ.   For senior officers and officials (one-star or equivalent and above), all requests to publish are to be referred to DMC for approval and may require a Ministerial Submission.

4.   **Planning Factors**   Requests for sponsored presences should be handled by Media and Communication staff, and should be judged on an assessment of risks and benefits, as with any other request for contact with the media. If given authorisation, planning for the sponsored presence should:

- Define the desired effects and supporting messages.
- Identify the content that would best deliver this effect.
- With the chain of command, carefully select the unit and/or individual.
- Convey the constraints (where and when recording/writing can take place)
- Assess sustainability and workload in keeping it up-to-date, including response to questions and comment;
- Convey the risks and subject areas to avoid;
- Formalise the process for production, clearance and review of the product.
- Establish the likely end date.

5.   **Style and Content**   Appendix I gives general guidance on written style and content. Media and Communications staff are to ensure personnel operating official presences have read and understood these guidelines. Sponsored presences will work best if they focus on that individual's contribution to the wider effort.

---

[12]   *Sponsored presences can be hosted on a corporate website (e.g. a blog within the RN, Army, RAF or MOD websites), on the website of a media partner (e.g. a blog written by a Serviceperson on a newspaper's website), be part of a wider social networking or similar site (e.g. a Serviceperson's page on a social networking site) or be hosted on a standalone personal site (e.g. a Serviceperson's own hosted and administrated blog).*

[13]   *This guidance does not address the creation of new corporate websites or .mod.uk addresses; see the guidance on Government websites set out in 2009DIN05-011.*

[14]   *For advice and to register a presence contact: [Redacted]*

6.   **Political Issues**   MOD and Service sponsored presences are not to be used to disseminate or advertise party-political information. Content generated for publication by or on behalf of Ministers must be approved beforehand by an official at Pay Band B2 (Grade 7) – or service equivalent or above.

7.   **Payment**   Personnel are not permitted to accept payment for material published as part of a sponsored presence.

8.   **External Comment**   In general, sponsored presences can carry external comments provided: this supports communication objectives, e.g. in establishing rapport and credibility with the audience; comments adhere to the guidelines at Appendix II; and, handling comments does not take up too much official time. Where MOD could be held liable for the content of external comments (for example comments on sites owned or hosted by MOD), they must always be pre-moderated (approved before they can appear). On sites not owned or hosted by MOD, external comments should be pre-moderated wherever possible. Operators of sponsored presences should be open about MOD's comment policy, which is at Appendix II.

9.   **Data Protection** Handling comments may involve holding personal data (e.g. names and email addresses of commenters). Operators of official presences holding personal data must observe the Data Protection Act 1998 (DPA98) and relevant MOD guidance.[15]

10.   **Questions**   Sponsored presence operators should aim to respond directly to questions online where an authoritative answer can be given quickly and simply. But such responses cannot be allowed to overwrite existing official channels of accountability (e.g., to Parliament) and should avoid being drawn into comment on issues outside their remit. Difficult or detailed questions (e.g., questions on policy issues or individual cases) should be referred to official channels:

- Where identifiable, queries from MPs or MPs' researchers should be answered through Ministers (via the Ministerial Correspondence Unit)
- When identified, press queries should be directed to the relevant press office.
- Questions outside the operator's field of expertise should be addressed to the policy lead for that issue, via the chain of command.

11.   **Freedom of Information (FOI)**   Some questions may qualify as FOI or Environmental Information Regulations (EIR) requests, whether they intended to or not.   Online presences should be monitored for questions that meet the FOI/EIR request criteria, but it should be made clear that if a formal reply is required, then a request should be made through normal FOI/EIR channels. A FOI request has the following characteristics:

- It must: Be in writing and legible (it can be electronic); contain the name and a return address of the applicant (an email address will do); and, describe the information requested;

- It need not: Mention the FOI Act or state the reason for the request.

12.   **Linking and Befriending**   Many online channels derive value by allowing one presence to be associated with others through linking, "befriending", and membership of groups. Membership of a wider network of online contacts can significantly increase the influence and effectiveness of a communication.   Sponsored presences can be associated with other presences, including unofficial presences, as long as these other presences are

---

[15]   *See the guidance "Comply with the Data Protection Act" on the Defence Intranet.*

people and organisations that you and your organisation would wish to be associated with in real life. Sponsored presences operated by individuals are permitted to make associations with presences from their lives outside work (for example family, friends, hobbies) where appropriate. Explicit endorsements of commercial products or services must be avoided,

13.   **Record-Keeping**   Sponsoring Commands are to ensure that records are kept of all material self-published to sponsored online presences wherever these presences are externally hosted. Sponsors should also keep copies of any external comments that were removed or disallowed.

14.   **Official Information**   Sponsored presences should NOT be used to store or communicate formal official information (e.g. official reports, statistics etc.) or to fulfil commitments to publish official information under Freedom of Information or other legislation. Such information belongs on the corporate MOD website (www.mod.uk).

ANNEX A - APPENDIX I: GUIDELINES FOR PERSONNEL OPERATING SPONSORED PRESENCES

Be clear about your aims:

- Think about what story you are trying to tell, to whom, and why.
- You are acting on behalf of your Service/MOD. Be open and honest about who you are, who you work for and what you are doing;
- Know your audience: what level of knowledge will they have? What will they be interested in?
- Understand the context in which you are contributing; respect the 'house rules' of the channel/forum/community.
- Avoid jargon or abbreviations unless you are certain your audience will understand them.

Be yourself and stick to what you know:

- Remember you are a member of HM Forces / MOD civil servant. Observe the same high standard of conduct and behaviour online as would be expected of you in your professional or personal life.
- Talk about things you have seen and done and know to be the case, rather than things you heard second hand.
- Stay in your lane and at your level. Stick to your job and your responsibilities.
- Do not comment on third parties without their permission.
- Express your thoughts and feelings, but make clear what is fact and what is comment.
- Be natural. If authorised to talk about work, don't change your style just because you're speaking "officially".

Engage with your audience:

- Answer direct questions quickly and simply if you can, and (if authorised) if it relates to your expertise.
- Refer more difficult or detailed questions about work to official channels (see Annex A Paragraph 10 "Questions" above for more details).
- Manage expectations of the level of engagement you are able to give. Don't feel you need to address everything anyone says. Admit it if you don't know the answer to a question, and keep any promises to find out.
- Don't be afraid to take a holiday from updates, or call it a day, if updating your online presence becomes too much work. Explain to your audience what is happening.

Make correct use of information:

- Use all and any interesting material you have, using pictures (still and/or video) wherever possible.
- Don't publish material you don't own, for example words, pictures or music lifted from elsewhere. Respect other people's copyright, and get relevant permissions for any material you use.
- Feel free to use links to authoritative sources of information, for example the Service and MOD corporate websites.
- Tag and label your contribution clearly so that other people can find it. Try to use tags that are meaningful to people who are not experts on what you do.

Think about reputation:

- Remember that you are representing your Service or the MOD, even if you are acting in your personal time.
- Do not post material others might find offensive, and avoid making bad comments about other people or organisations.
- Think about your personal reputation. Don't publish anything you wouldn't be happy for your parents or your children to see.
- Always think about the wider impact of what you publish. It will be there for all to find, and could attract media attention. If you have any doubts, take advice from your Chain of Command/Line Management.

Maintain security:

- Familiarise yourself with the security risks and remedies described in Annex C.
- Do not take risks with Operational Security (OPSEC).
- Do not risk your personal security (PERSEC) by publishing anything that could be used to blackmail, threaten or embarrass you.
- Maintain the security and respect the privacy of colleagues and their families. Don't publish information about them without their permission.

And in general:

- If ever in doubt over whether to publish something, always consult your Chain of Command/Line Management.
- Enjoy yourself – You have a great story to tell, and are the best person to tell it.

ANNEX A - APPENDIX II: MOD ONLINE EXTERNAL COMMENT POLICY

1.   It is MOD policy to allow comments by external users on selected corporate and sponsored web presences where this supports wider Departmental objectives, for example by enabling better engagement with our readers.

2.   We ask that comments by external users on official MOD presences follow the same guidelines as apply to our own staff when they use official IT. These internal MOD guidelines are set out in Joint Service Publication 740 (MOD IT Acceptable Use Policy), and are updated periodically.

3.   In summary, these guidelines state that you must not knowingly transmit:

- offensive, indecent or obscene material or abusive images and literature
- material which can reasonably be considered as harassment of, or insulting to, other people or organisations;
- material obtained in violation of copyright or used in breach of a licence agreement;
- spam (electronic junk mail) or chain email;
- material that could, by their presence on an MOD website, reasonably be expected to embarrass or compromise the MOD (although comments that disagree with the MOD are allowed).
- commercial activities which are not connected to MOD business;
- any form of gaming, lottery or betting;
- any form of share dealing;
- offers of items for sale or bids on commercial auction sites;
- chain schemes (such as pyramid selling);
- material designed to mislead people about who originated or authorised it (e.g. through misuse of signatures);
- attempts to compromise MOD IT and Telecoms, prevent legitimate access to them, damage them or seek to cause degradation of performance or a denial of service;
- attempts to gain unauthorized access to MOD IT and Telecoms or content for which you do not have permission (i.e. Hacking);
- attempts to access, amend, damage, delete or disseminate another user's files, emails, communications or data without the appropriate authority.

4.   We will withhold, edit or remove any comments we judge do not follow these guidelines.

5.   Opinions expressed in comments are those of the author not those of the MOD. The use of comments does not overwrite the existing, official channels by which the Ministry of Defence and the Armed Forces are held accountable to Parliament and to the Public. Nor does it affect your rights under the law, for example your right of access to official information under the Freedom of Information Act 2000.

6.   We will respond directly to questions and queries online where an answer can be given quickly and simply. More difficult or detailed questions (for example, questions concerning policy issues or individual cases) should be referred to existing official channels of accountability, such as writing to your MP, asking a Defence Minister or making a Freedom of Information request. Press queries should be directed to the Defence Press Office.

7.   The MOD reserves the right to ignore, limit or suspend comments or responses to comments, locally or universally and without prior notice, if we judge that these are becoming a waste of official funds, or Armed Forces' or Civil Service time.

ANNEX B: GUIDANCE FOR SERVICE AND MOD PERSONNEL WHEN ONLINE

This guidance is for Service and MOD civilian personnel making personal use of the internet and applies to any engagement with any website, blog, photo or video channel, bulletin board or online forum, social network, wiki or multiplayer game.

- Service and MOD civilian personnel are expected to adhere to the same high standards of conduct and behaviour online as they would in any other aspect of their professional or personal lives.
- Be aware of the dangers to yourself and others in sharing information online. Always maintain personal, information and operational security. It is essential that all staff follow the security guidance at Annex C and seek advice from their chain of command if in any doubt
- You are allowed to identify yourself as a Serviceperson / MOD civilian, for example in a user profile or photograph. This can include stating your trade or occupation with the Services/MOD, subject to the security guidance at Annex C and any local security guidance (for example, any connection with SF or NI must not be disclosed).
- Don't publish information about third parties (including colleagues) without their permission.
- You do not need to seek clearance to publish material not connected with your work, for example material relating to your personal hobbies and interests.
- You must seek authorisation before publishing any wider information relating to your work which:
  ◦ reflects on wider Defence and Armed Forces activity;
  ◦ attempts to speak, or could be interpreted as speaking on behalf of your Service or the MOD;
  ◦ or, relates to classified[16], operational, controversial or political matters.
- Consider using or referring to material on Service and MOD corporate websites in your conversations.
- Think about your personal reputation. Don't publish anything you wouldn't be happy for your parents or your children to see.
- You are not prohibited from expressing views (for example, on a bulletin board, joining a campaign or signing a petition) but should avoid being drawn into making attributable comments on controversial matters.
- When taking part in a campaign you should not use your rank (i.e. use Mr Smith not Major Smith) or indicate you are a MOD Civil Servant, as this could be taken by other readers as official endorsement.
- If you wish to start a poll, petition or other campaign which relates to Defence or Armed Forces, seek permission first.
- You are not prohibited from editing Wikis if you have useful information to contribute, but you should avoid attempting to edit material relating to your work "officially" unless authorised.
- You can act anonymously or pseudonymously in a personal capacity where appropriate but must (i) still follow this guidance (ii) be aware that very few things on the internet are genuinely anonymous and most can be traced, potentially by someone hostile and (iii) understand that Service, MOD and other authorities will pursue serious breaches of the rules, regardless of whether the person intended to publish anonymously.
- Consider volunteering to operate a "sponsored" online presence if you believe your work is worth sharing with a wider audience.
- If unsure, always seek advice from your Commanding Officer or Line Manager before going ahead.

---

[16]   Protectively-marked at PROTECTED or RESTRICTED or above, or caveated e.g PERSONAL or STAFF.

ANNEX C: GUIDANCE ON MAINTAINING SECURITY ONLINE

See JSP 440 "The Defence Manual of Security" for further information and advice on maintaining security.

The threat to your information

Below are the main categories of information that could be at risk, the hostile groups that might seek this information, and the potential consequences if this information is compromised.

Personal Information is always at a premium in the criminal and espionage world. Items of information which can be used to take advantage of you and your family can include:

- Full Name
- Date and Place of Birth
- Full Home Address
- Telephone Numbers
- National Insurance Number
- Passport Details

Information such as this may also enable hostile intelligence agencies or terrorists to target you or your family. You should protect this information from open publication.

It is possible to give away information about yourself unintentionally through the linkages you make with other people. For example, by looking at your friends on a social networking site it would be fairly easy for a stranger to work out roughly where you live and your approximate age – even if you have not volunteered any of this information yourself.   This makes it even more important to safeguard the exact details of your personal information described above.

Account details Criminal groups may also try to gain access to online, telephone or other accounts using your account details. This includes information such as:

- Account Numbers
- Logins / User IDs
- Passwords
- PIN Numbers
- Memorable Phrases
- Security Questions

Information such as this could be used for criminal activity or blackmail.   Do not give out this information to third parties.

Details about your work   Hostile intelligence services or terrorist organisations may seek details about your work or your unit/establishment. This may include:

- Establishment/Unit Location
- Work telephone Number
- Rank/Staff/Service Number
- Position/Role

Information such as this could enable your Establishment/Unit to be targeted. Protect this information and specifically, do not disclose:

- Any protectively-marked or caveated information.
- Any connection to Northern Ireland, or information on people connected to the Armed Forces domiciled in Northern Ireland.
- Any connection with, or mention of, Special Forces or supporting elements.

Images can give away important information unintentionally. Check to make sure Forces ID cards, Official passes, keys, computer screens, paper documents or other potentially sensitive materials or equipment are not visible.

Operational information If you are involved in operations directly or supporting them, information protection becomes even more important and attempts to gather information by hostile agencies or groups may become more determined. Information that will be of interest to these groups includes:

- Operational Programme
- Deployment Details
- Capability Shortfalls
- Casualty details
- Morale
- Mission-Specific Information

Information such as this can be used by an enemy in countering our operations, putting lives and assets at greater risk. It may also damage our credibility with our allies and possibility lead to a withdrawal of their support. Do not release it online.

Protecting your information

As well as withholding the types of information described above, there are a number of simple steps you can take to protect yourself online:

- Understand and apply your security settings.
- Choose your online friends carefully and be circumspect in the information you share with them.
- Only post items that would be acceptable to your family, friends or colleagues.
- Make sure photographs don't give away information you want to protect.
- Do not give out unnecessary information when registering.

To maintain security on the web the following is general good practice:

- Do not share your logins or passwords.
- Change passwords regularly.
- Use a password that would be difficult to guess – don't use simple words and mix upper- and lower-case characters, and numerals.

Protecting your friends' and colleagues' information

Some social networking sites enable you, indirectly, to publish information about other people, for example by identifying them in photographs. Be careful about disclosing information about friends and colleagues. Respect their privacy and maintain their security.

- Breaching the rules on the handling of other peoples' personal information is a disciplinary and potentially criminal offence.

- Take care not to disclose personal information about your friends and colleagues that they might want to keep private, for example medical or family problems or forthcoming deployments.
- Be wary of publishing group photos or course photos which link individuals to organisations. Are all the people in your photograph happy to be identified?
- Exercise particular care in posting photographs or other information about third parties working with the Services or MOD, such as interpreters or locally-employed staff. You could inadvertently place them at risk.

If you suspect information has been released in error

Security is everybody's responsibility. Our own personnel are our eyes and ears on the Internet. If you see information on the Internet that falls into one the categories above, that you suspect may have been released without proper authorisation, contact your Commander or Line Manager immediately so that mitigating action can be taken.

If information of a sensitive, personal and operational nature is exposed into the public domain, Commanders and line managers should report the incident up their chain of command, to their Branch Security Officer, and (via the BSO if available) to the Joint Security Co-ordination Centre[17] (JSyCC). Neither Commanders nor staff should attempt to remove third party material from the Internet without authorisation and advice from the relevant security authorities.

---

[17] JSyCC contact details: *[Redacted]*