#DIGITALARMY

USING SOCIAL MEDIA IN THE BRITISH ARMY

Version 1: 1 September 2018[1]

ARMY
BE THE BEST

WHY DO WE HAVE THIS POLICY?

Like the rest of UK society, we in the Army are ever more connected through smart technology to conduct our everyday lives, keep in touch and create our online presence. When we use online services or interact with social media we generate a digital footprint that can be a force for good, but can also be exploited by those who wish the Army, soldiers or their loved ones harm or to tarnish our hard-won reputation.

Social media offers the Army fast, direct communications within its workforce as well as highly effective ways of communicating externally. Research shows that some of our best received communications are created by more junior ranks using digital channels in an authentic manner. The Army is keen to support them. Many of our soldiers and officers are blogging and posting videos and articles online in a way that is encouraging healthy debate about the Army and informing the public about what to expect if they join our ranks. We want to expand this and demonstrate that the Army is open, diverse and welcomes all. However, with digital communications come significant responsibilities. The Army is a national institution that protects the UK; its reputation must be looked after to preserve its credibility as a fighting force, its freedom to operate and its attractiveness as a modern employer that fulfils its people's potential.

Our digital footprint can be a force for good

This document has therefore been written to provide a 'one-stop shop' for anyone who works for the Army and to that end it is aligned with the MOD's IT Acceptable Use Policy[2] and the DIN Contact with the Media and Communicating in Public[3] issued by the Directorate of Defence Communications (DDC). **It includes advice about maximising the effect of your online communications as well as describing the behaviours expected by the Army when using social media.** The addition of the word 'social' does not stop these channels being public communications.

WHO DOES IT APPLY TO AND WHEN?

Like the Army's Values & Standards, this policy applies to all members of the Regular and Reserve Army, whether on duty, off duty or on leave, and whenever they use social media. It does not matter whether you are communicating in a personal capacity, in public or just with colleagues, at work or outside. More stringent rules apply to social media accounts that are clearly operated by an Army 1-star or above. This policy also applies to Civil Servants working for the Army, whose behaviour is subject to the Civil Service Code.

HOW TO USE SOCIAL MEDIA TO BEST EFFECT

Not everyone in the Army uses social media in the same way (or at all) but the reality is that most of our workforce will have personal accounts on one or more social channels. In addition, many appointment holders (eg Commanding Officers, Regimental Sergeant Majors, Brigade Commanders, General Officers Commanding, ECAB Directors, Defence Attachés/Advisers) have one or more official accounts. This guidance reflects today's civilian workplace best practice, but has been enhanced to accommodate the particular challenges associated with Defence.

[1] This policy supersedes ABN 86/13 dated 3 Sep 13 but is aligned with the AMC Digital Strategy dated 8 Jan 16.

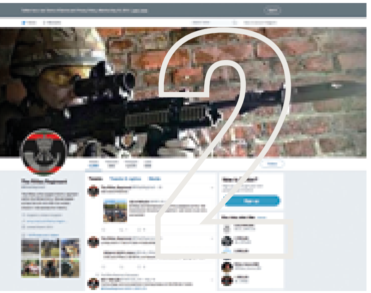
[2] Laid out in JSP 740 and required to be signed before using MOD IT systems. https://www.gov.uk/government/publications/acceptable-use-policy-jsp-740

[3] https://www.gov.uk/government/publications/defence-instruction-contact-with-media-and-public

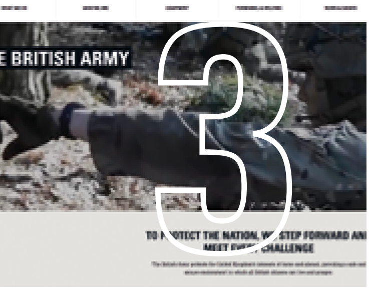
WHAT ARE THE DIFFERENT CATEGORIES OF SOCIAL MEDIA USED IN THE ARMY?

The Army puts social media use into 3 categories:

Personal online presences are those operated by individuals in their private lives and outside their official duties and include: websites, blogs, vlogs, bulletin board accounts, social network and dating site profiles, private messaging, wiki or multiplayer game avatars.



Official online presences are approved and *registered* with Army Media and Communications (AMC) and *operated* by individuals, units or formations in a deliberate and coordinated fashion to communicate the Army's and specific unit or formation messages. They are designed to engage with public audiences at a more personal, informal level but with the official approval of the Army.

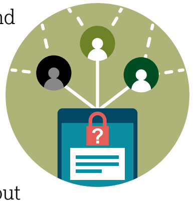

3
BRITISH ARMY
TO PROTECT THE NATION, WE STEP FORWARD AND MEET EVERY CHALLENGE

The Army's **corporate** online presences are operated by the communications professionals in AMC and include: the official Army Website, Army Facebook, Army YouTube, Army Twitter, Snapchat and Instagram accounts. In addition, Army Recruiting and Initial Training Command is responsible for the Army's recruiting website.

SET YOURSELF UP PROPERLY

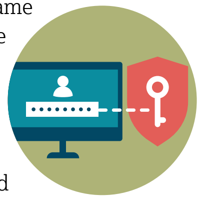
OPERATIONAL AND PERSONAL SECURITY

- While social media offers an excellent means of communicating with friends and colleagues, it also presents serious threats to security. You must not publish anything that threatens any individual's personal security or breaches operational security. When communicating on social media:
  - Photographs of yourself and colleagues in uniform or in obviously Army locations may not always be advisable - think carefully before posting them.
  - Do not post details about your work that could be used by criminals, terrorists or potential enemies to harm you or your colleagues.
  - Remember, even a restricted online profile, visible only to 'friends', can be easily accessed by uninvited third parties.
  - Turn off geo-tagging on devices to prevent your location from being revealed.
  - Stop posting in the event of a major incident, especially if colleagues have been injured or killed or if 'Op MINIMISE' has been imposed.
  - **Contact the Warning Advice and Reporting Point (ArmyWARP-Mailbox@mod.gov.uk or 01264 886803/4) for security advice or to flag up a possible or actual cyber security incident.**



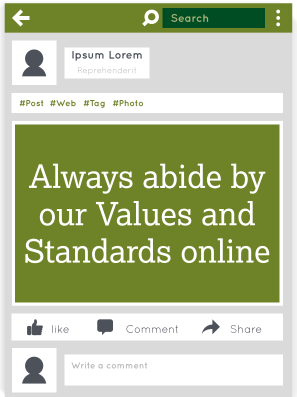
HAVE YOUR SAY, SECURELY

- Nothing in cyberspace should be considered private. This applies to private messaging services such as WhatsApp or Facebook Messenger just as much as to sites such as Facebook/Twitter and their publicly posted content.
- Do not expect anonymity even if using a pseudonym for your account. Consider how a third party might read or use your posts.
- Do not expect or rely on the security of online communications. Think about the security and data protection implications of anything you post - don't post any personal information, either your own or anyone else's.
- You may be held responsible for communications in cyberspace, on the Internet or in social media, even if those communications go beyond the audience/recipients you intended.
- Read other people's posts carefully before liking, reposting or responding to them. Be on the look-out for 'fake news' and phishing.
- Regularly check and update your social media settings. When apps or software update, they often reset to default settings.
- Maintain good password security: use at least 8 characters with numbers, letters and symbols; do not use personal information such as your date of birth or mother's maiden name; do not use the same password across multiple sites as it makes identity theft easier; and do not share passwords - your trusted friend today might not be your friend in the future.



PERSONAL ACCOUNTS

- If you're going to use social media in a private capacity, apply the principle of 'do no harm' and the following guidance to your personal accounts:
  - You do not need permission to use social media for personal and occasional, low-key Army social events, but should inform your chain of command if you wish to communicate *regularly* about Army activities. Making your account 'official' would then probably be more appropriate.
  - Access your personal social media accounts on your personal device rather than one issued by the MOD.



Always abide by our Values and Standards online

  - Think carefully before indicating in online profiles such as for social networks or dating sites that you are in the Army. However, if you choose to be public, the Army fully supports anyone who contributes positively to our overall digital presence.
  - Whether your profile indicates that you are in the Army or not, your posts and videos must always abide by our Values & Standards and be clear that you are **not** communicating on behalf of the Army in an official capacity.
  - If you 'go public', think twice about using your rank and do not put Army badges or our logo in your personal account profiles – they are reserved for official and corporate accounts.
  - Signing an online petition as a private citizen is fine, but always ask permission if you would like to start a poll, petition or campaign about the Army or Defence.
  - If you think you are posting something worthy of being re-posted on the Army's corporate channels, let your Unit Press Officer know in advance to exploit other channels and reach the widest audience.
  - Online defence forums have international reach and are monitored by other armies and journalists. Assume that any posts you make will be picked up, re-posted and aired on mainstream channels. Anonymity is not a safe assumption.
  - While you are not responsible for content posted by online groups that you are a member of, inappropriate content can be linked to you and then to the Army. The Army supports you if you stand up for our message online, but it is better never to be associated with inappropriate content.
  - Do not use personal social media accounts such as Whatsapp or FaceBook for routine Army work such as Part 1 or sub-unit orders, sports teams and so on – they are not secure and it may breach data protection laws. Use Defence Connect, the jive daily app or MODNet Skype for Business instead.
  - Be upfront if you make a mistake online. It is virtually impossible to take something back, even if you delete it quickly, so it is best to tell your boss if you have got it wrong.
  - Help colleagues by looking out for inappropriate postings. If you think someone should take something down, message them privately instead of drawing attention to it publicly.
  - If you set up an anonymous personal account or use a pseudonym you must still follow all the guidance above. Remember - very few things online are genuinely anonymous and everything can be traced by the police.
  - Do not create fake accounts to impersonate other people – it is illegal, breaks social media site rules and is against Army policy.

OFFICIAL ACCOUNTS

- You need an official account if you intend to post regularly about your work in the Army. Here is what you should know:
  - All such accounts must be approved by and registered with the AMC Digital Team, who will help you set up the account name, your profile picture and settings for best impact and appropriate security. They will also advise on tone of voice, approach and content.
  - If you have one, use an issued MOD device to access your official social media accounts.
  - If you are using a personal device for official accounts, ensure its integrity by protecting access to it with a password or fingerprint and keeping anti-virus software up to date.

Official accounts must carry the Army branding

- Your account needs to carry our official branding. Usually this will be your unit or formation badge (available from the Army Brand Portal[4]) but you could alternatively ask to use the Army logo (fluttering Union flag + *Be the Best*). Seek advice from AMC Digital.
- Have a plan and SMART[5] objectives for how you intend to use your official account(s); running channels such as Twitter and Instagram is time-consuming and you will need to allocate part of your day to maintain your social media's effectiveness.
- Read the Army Communications Plan[6] and understand the Army's Communications Objectives. If your official social media posts do not fit one of those objectives you will not be messaging effectively for your unit and the Army. However, if done well, the Army's network of official accounts offers great opportunity for message amplification and reinforcement.
- Follow the tips in the Army Digital Playbook[7] to gain the greatest reach and impact from each of your posts.
- Tag and hashtag the Army into interesting events, pictures, videos and posts and re-post other official Army accounts to amplify our messages. But be very selective about who else you 'like' or re-post, especially if they are not 'blue ticked' accounts.
- AMC's Digital Team will re-post the best posts they see on official accounts and will pass them on to the MOD's Digital Team, too. If you think you have posted something particularly good, let them know.
- You must remain politically and diplomatically neutral and must not be seen to use an official Army account to promote any commercial companies or products or fund-raise.
- Always be very careful when posting pictures of children; unless you have the explicit permission of their parents or guardians do not use them.
- AMC will monitor your account to measure its success and are there to help you improve the quality and reach of your posts.

[4] https://defencebrandportal.mod.uk/BMS/index.cfm

[5] Specific, Measurable, Attainable, Result-orientated, Time-bound.

[6] https://jive.defencegateway.mod.uk/docs/DOC-157359

[7] https://jive.defencegateway.mod.uk/docs/DOC-157359

RESPECT OTHERS AND THE LAW

- Post on social media as if you were face-to-face with your audience. Use good judgement, do not break the law and always apply the Army's Values & Standards, whether you are using an official or a personal account.
- It is fine to disagree with someone else's opinion online but not to make negative comments of a personal nature.
- Respect and have pride in your colleagues and their work. Do not undermine the Army or your part of it. **Like any employer, the Army expects those working for it to support it** so think carefully about the fine line between constructive criticism and 'sounding off' unprofessionally.
- If you're setting up a social media group in your workplace, whether using a personal or official account, include people fairly and never discriminate against anyone.

Respect and have pride in your colleagues and their work

- Debate is good, a protracted online argument is not. It is better to disengage than get into a downward tit-for-tat post spiral. This is particularly important if a thread has become political or derogatory, has started to include extremist views or has crossed the bounds of OPSEC or our Values & Standards.
- Do not comment on any ongoing court case or court martial – you risk contempt of court charges.

- The Army takes 'trolling' of your line management or peers as seriously as any civilian employer; it is contrary to our Values & Standards and could also be a criminal offence. Do not naively assume that a post to an online forum such as ARRSE or Fill Your Boots under a pseudonym will go unchallenged.
- Posting and viewing images of a sexual nature online is fraught with risk, even when it is between consenting adults. It is easy to lose control of digital images and just as easy to break the law unintentionally. Viewing indecent images of anyone who is or appears to be under the age of 18 is illegal, regardless of how old they look.
- Do not post anything that breaches copyright or that is inflammatory, offensive, harassing, defamatory, demeaning or provocative. However angry you may feel about a thread, do not deliberately de-rail an ongoing debate.
- When using official accounts or undertaking official business, posting of other people's personal data without their consent, which includes 'tagging' them, may breach the Data Protection Act 2018 and could be referred to the Information Commissioner.
- Challenge any Army colleague, Civil Servant, contractor working for the Army or ex-military who posts something that you feel is contrary to our Values & Standards. Alternatively, inform your chain of command so they can deal with it.

Remember - the way you act online should not be different from how you act in person. Help to spread and enhance the Army's messages online as you would in person. Online behaviour which adversely affects the reputation of the Army or which undermines morale, good order, discipline, trust may be considered a breach of the Service Test[8] and lead to Major Administrative Action. Illegal behaviour online will be dealt with through disciplinary procedures or by the civilian police and courts.

[8] Further guidance on the Service Test is at Ch 067.020 to AGIA 67.

The Values and Standards of the Army are our internal employees code, which underpins the Army brand.

RESPECT FOR OTHERS COURAGE LOYALTY

DISCIPLINE INTEGRITY SELFLESS COMMITMENT

ACCEPTABLE BEHAVIOUR TOTALLY PROFESSIONAL LAWFUL

Creative Media Design
ADR007595

AC64659