GUIDELINES ON THE SAFE USE OF THE INTERNET AND SOCIAL MEDIA BY MDP OFFICERS

The Association of Chief Police Officers (ACPO) has recently agreed and published guidelines to all police forces in England, Wales & Northern Ireland on the safe use of the internet and social media. For HO Forces, the guidelines relate to police officers and police staff.

The guidelines have now been amended and incorporated for use in the Force and apply to all officers in the MDP including Scotland.

The purpose of this document is to assist MDP officers and the Force to make good decisions and act responsibly. This will be in a manner that will allow them to make effective and safe use of the Internet and social media during working hours and in their private lives.

The document will be updated and re-published as necessary.

Any queries relating to this document should be directed to Hd PSD.

SECTION 1 - INTRODUCTION

1. The exponential growth in the public use of Social Networking Sites (SNS) over the last few years has provided significant new opportunities to make contact with others. These opportunities come in different ways.

2. Professional Standards readily acknowledge the benefits of such new ways of communicating but many cases have been documented when officers fail to understand the dangers of SNS - both to themselves and their families and to the Police Service. What was once a private domain of communication has become one that is very much public

3. This advice has been created with the intention of informing police officers of the challenges such SNS sites present. By following the guidance, the Force and officers will be better informed and able to provide the professional service the public wants from us all.

SECTION 2 - AIMS

4. ACPO encourages the Police Service to embrace the many benefits available through effective use of the Internet and social media. Such benefits can include more effective communication with communities, more informed consultation and local engagement, and an opportunity to demonstrate greater accountability and transparency. Further advice to police forces is available within the ACPO and NPIA publication *'Engage: Digital and Social Media Engagement for the Police Service'.*

5. Alongside the benefits of such digital engagement there is however some risks to personal and organisational security or reputations which, although significant, can be managed to acceptable levels provided the Force and police officers are aware of the risks and act responsibly.

6. These guidelines are intended to assist police officers and the Force to make good decisions and act responsibly in a manner that will allow them to make effective and safe use of the Internet and social media during working hours and in their private lives.

SECTION 3 – GENERAL GUIDANCE

The same standards of behaviour and conduct apply online as would be expected offline.

7. Information placed on the Internet or social media could potentially end up in the worldwide public domain and be seen or used by someone it was not intended for, even if it was intended to be 'private' or is on a closed profile or group. It is likely that any information placed on the Internet or social media will be considered to be a public disclosure.

8. The public expect police forces and police officers to act with integrity and impartiality whilst upholding fundamental human rights and according equal

respect to all persons. Police officers must abstain from any activity that is likely to interfere with the impartial discharge of their duty, or to give the impression to the public that it may interfere and must abstain from any active role in party politics.

9. Police officers should avoid using the Internet and social media off duty after consuming alcohol or when their judgement may be impaired for other reasons.

10. The use of social media for private purposes during working time and from Force systems should be in accordance with Force policies. The use of social media for such purposes during working time, and from personal mobile devices, is not recommended.

11. Officers should be familiar with force policies and procedures covering topics such as Information Security, the Data Protection Act 1998, and use of force intranet and e-mail.

SECTION 4 - CATEGORIES OF RISK

12. The safe use of the Internet and social media requires an awareness of risks across five areas:

a. Breach of trust or confidence - disclosure of information obtained by the police service, about the police service, or about colleagues

b. Unauthorised disclosure of personal data - breach of the Data Protection Act 1998

c. Bringing discredit on the police service - on or off duty conduct which affects public confidence

d. Revealing personal information - increased vulnerability to harassment, corruption or blackmail, and

e. Revealing operational material or tactics - prejudicial to investigations

These categories are explained in more detail below.

SECTION 5 - MAINTAINING THE TRUST AND CONFIDENCE OF OUR PUBLIC

Risk category A: Breach of trust or confidence.

CONFIDENTIAL INFORMATION

13. Police officers and the force in general have a legal duty not to disclose information obtained from third parties through the conduct of

their official duties. Such information must not therefore be posted on the Internet or social media.

14. The public would be discouraged from confiding in the police service if they did not have a degree of certainty that information provided in confidence would be respected. A detailed explanation of the duty not to disclose information provided or obtained in confidence, and limited exemptions which may apply, are contained within the related guidance from the Information Commissioner's Office available online at:

http://www.ico.gov.ukupload/documents/librarv/freedom of information/detailed specialist guides /awareness guidance 2 - information provided in confidance.pdf.

15. The MDP Standards of Professional Behaviour applies to MDP officers and provides:

- Police officers treat information with respect and access or disclose it only in the proper course of police duties.

- The force shares information with other agencies and the public as part of its legitimate policing business. Police officers never access or disclose any information that is not in the proper course of police duties and do not access information for personal reasons. Police officers who are unsure if they should access or disclose information should always consult with their manager or the MDP Data Protection Officer before accessing or disclosing it.

- Police officers do not provide information to third parties who are not entitled to it. This includes for example, requests from family or friends, approaches by private investigators and unauthorised disclosure to the media.

ORGANISATIONAL INFORMATION

16. It is recommended that police forces provide officers with a method of communicating adverse comment, dissatisfaction or frustration in relation to organisational matters for the attention of senior management. Such facilities may include internal forums or chat rooms hosted on force Intranets.

17. Police officers are advised not to make adverse comment regarding their police force, colleagues or senior managers, or the police service in general on the internet or social media and are advised to make use of internal facilities to vent any such comments.

18. ACPO and the Force encourages all police officers to make use of confidential and independent reporting services to provide information on alleged illegal, corrupt, misconduct or discriminatory practices within the organisation. The PSIU confidential reporting line is available for this purpose.

19. Further details of the protection that police forces will afford police officers and others who provide such information as 'whistleblowers' is contained within the Public Interest Disclosure Act 1998.

SECTION 6 - SAFEGUARDING PERSONAL & SENSITIVE DATA

Risk category B: Unauthorised disclosure of personal data.

UNAUTHORISED DISCLOSURE OF PERSONAL DATA

20. Police officers and the Force have access to a significant amount of personal and sensitive data which is protected under the Data Protection Act 1998.

21. Personal data means data which relates to a living individual who can be identified:

- From the data, or
- From the data and other information which is in the possession of, or is likely to come into the possession of the data controller or any other person in respect of the individual and includes any expression or opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

22. Sensitive personal data means personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence, or
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

23. Police officers who obtain personal data or sensitive personal data about third parties in the course of their duties and disclose that data without authority on the Internet or social media are likely to have committed a criminal offence.

SECTION 7 - MAXIMISING THE REPUTATION OF THE POLICE SERVICE

Risk category C: Bringing discredit on the police service.

BRINGING DISCREDIT ON THE POLICE SERVICE

24. Discredit can be brought on the police service by an act itself or because public confidence in the police is likely to be undermined as a result. In the interests of fairness, consistency and reasonableness the test as to whether conduct has brought discredit on the police service must have regard to all the circumstances and not solely media coverage.

25. Police officers should be mindful of the viral effect of the Internet and social media and the potential for the smallest piece of information to be up scaled beyond all expectations.

26. In determining whether an individual's off-duty conduct discredits the police service, the test is not whether the individual discredits herself or himself but the police service as a whole.

27. The MDP Standards of Professional Behaviour applies to MDP officers and provides:

- Police officers behave in a manner which does not discredit the force or undermine public confidence, whether on or off duty.

28. ACPO acknowledges that police officers have rights to Freedom of Expression under Article 10 of the European Convention on Human Rights (ECHR) but reminds all officers that such rights are restricted.

29. The expression of views or conduct which appears to support discrimination against any group, or encourages racial, religious or homophobic hatred will not be tolerated.

30. Police officers are advised not to make any comment or post any images of behaviour on the Internet or social media which are, or could reasonably be perceived to be, beliefs or conduct that are contrary to the expectations of behaviour outlined in Police Standards of Professional Behaviour.

SECTION 8 - KEEPING YOUR PRIVATE LIFE PRIVATE

Risk category D: Revealing personal information.

REVEALING PERSONAL INFORMATION

31. Criminals and others may seek to use the Internet and social media to identify personal information about police officers with a view to embarrassing, discrediting, harassing, corrupting or blackmailing them or their families for

their own benefit.

32. Police officers in rural locations, in sensitive posts, with uncommon names, or in high profile posts are particularly vulnerable to such attempts.

33. It is recommended that police officers:

- Remove personal details from the edited electoral roll
- Ensure telephone numbers are ex directory
- Opt all family members out of online commercial search facilities such as 192.com
- Ask 'Google maps' to remove pictures of their house, car or persons from their site http://www.ehow.com/how S723475 remove-street-photos-google.html
- Register to avoid unwanted telephone via http//www.tpsonline.org.uk/ctps/number
- Register to avoid unwanted mail via http://www.mpsonline.oro.uk/mpsr/mps
- Ensure privacy settings for social media are set to the highest level
- Do not register on social media using pnn.police.uk e-mail addresses
- Are careful when accepting 'friends' to access their social media
- Are not associated with inappropriate material on 'friends' social media
- Are not associated with social media of criminals
- Are not associated with the social media of persons involved in serious organised crime
- Remember that online users may not be who they purport to be
- Ensure all computers and mobile devices have up to date security and anti virus software installed
- Use strong passwords and never share them
- Shred all paperwork containing personal details
- Contact PSIU if they become subject of online abuse linked to their occupation, if a 'spoof social media account is established purporting to be used by them, or if their genuine social media account is 'cloned', 'hacked', or 'taken over' and;
- Read the gener**al online safety advice at:**

http://www.getsafeonline.org/media/getsafeonline roughguide.pdf

34. It is recommended that police officers do not post any of the following information on the Internet or social media:

- Details of your employer
- Details of your post
- Images in uniform
- Mobile telephone numbers
- Home addresses
- Personal e-mail addresses
- Family members' details
- Hobbies and places frequented
- Details of vehicles
- Sensitive personal data as outlined at paragraphs 16-19
- Images or details of colleagues without their consent

35. It is recommended that police officers:

- Do not advertise work related social events on the internet of social media
- Use internal intranet for all work related social notices, and
- Vary premises frequented for work related social events

36. It is recommended that police officers in sensitive posts, as defined by a requirement for 'Management Vetting' or 'Developed Vetting' clearance, carefully assess all risks associated with the use of personal social media accounts and maintain an awareness of the content of family members' social media accounts.

37. It is also recommended that police officers who may wish to pursue duties in covert policing carefully consider whether the publication of personal images and information on social media may restrict their future career opportunities in such areas on the grounds of personal safety, public safety and operational security.

SECTION 9 - MAINTAINING PUBLIC SAFETY

Risk category E: Revealing operational material or tactics.

REVEALING OPERATIONAL MATERIAL OR TACTICS

38. The police service has a duty to prevent and detect crime, prevent disorder, protect vulnerable communities and preserve the rights of individuals.

39. In order to carry out such duties the police service requires an ability to develop, plan and carry out operational activities secure in the knowledge that such matters will only be divulged to police officers, police staff and other persons with a legitimate 'need to know'.

40. Tactics used by the police service, including covert tactics, must remain matters for the police service if they are to remain effective and serve the interests of the public.

41. The disclosure of information relating to ongoing criminal prosecutions or persons involved in such matters is strictly controlled by law as it may compromise the rights of an individual to a fair trial under Article 6 of ECHR. Such disclosures may also amount to a Contempt of Court.

42. The unauthorised disclosure of operational and tactical information can have serious consequences for public safety, can reduce the effectiveness and efficiency of the police service in general and is a serious criminal offence.

43. The Official Secrets Act 1989 provides that, in summary, any police officer or member of police staff is guilty of an offence if, without lawful authority they disclose any information, document or other article, the disclosure of which:

- Results in the commission of an offence
- Facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody
- Impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders, or
- Such that its unauthorised disclosure would be likely to have any of those effects.

44. Police officers must not reveal operational material or tactics on the Internet or on social media.

45. The use of mobile internet devices and 'smart' phones with an ability to access the internet and social media may cause police officers to inadvertently disclose operational material and tactics.

46. With advances in digital technology, images obtained using 'smart' phones' contain data revealing the exact geographical location where the image was captured. The subsequent posting of such images on the internet or social media makes it relatively easy for personal or operational information to be disclosed unintentionally.

47. Location Based Services (LBS) allow social media allows users to 'check in' to a particular location, to learn which other social media users are at the same location, and, for example to earn points or discounts from retailers.

48. Readily available LBS social media applications allow anyone to track the movements of other persons using LBS to the extent that identification of current location, home address and place of work is easily identified from patterns of movement.

49. Police officers deployed on covert or other operations are strongly advised to disable LBS and GPS services on personal 'smart' phones and to avoid the unintentional disclosure of their location through the posting of images on the Internet or social media.

50. It is recommended that police officers and staff are very careful should they choose to allow LBS and/or GPS services to operate on their 'smart' phones whilst off duty.

51. Further information on the risks associated with LBS and GPS services on 'smart' phones will be available from force Operational Security Advisors or similar post holders or from: http://consumers.ofcom.org.uk/2009/10/a-guide-for-parents-and-carers-on-mobile-location-based-services/.

SECTION 10 - CONCLUSION

52. The internet and social media offer can offer significant benefits and services to police officers but they are not without risk.

53. ACPO encourages all members of the police 'family' to take advantage of those benefits but to do so responsibly and in a manner that reduces risks to an acceptable level.

54. Please make full use of the internet and social media but please do responsibly.