WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	SOCIAL and DIGITAL MEDIA POLICY.
POLICY REFERENCE NO:	CC/01

Executive Summary.

The purpose of this policy document is to set out to all officers and staff the definitive Force corporate approach to the use of social media accounts i.e. Twitter, Facebook, YouTube, Snapchat, Instagram, Flickr, LinkedIn and blogs etc in line with their work. It defines the procedures for applying for a corporate account, its management thereof and the critical security and safety procedures relating to both the recording/loading of information, and loss of associated equipment.

In addition, the policy will also remind all officers and staff about the personal use of social media, its potential security threats and legal responsibility regarding the inappropriate use or disclosure of such sites.

**Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Intended Policy Audience.

This policy is primarily aimed at all police officers and staff of West Midlands Police.

Current Version And Effective Date.	**Version 2.1**	**23/05/2019**
Business Area Owner	**Corporate Communications Department**	
Department Responsible	**Corporate Communications Department**	
Policy Contact	**Dan Barton**	
Policy Author	**Mike Woods**	
Approved By	**Mr D. Thompson – Chief Constable**	
Policy Initial Implementation Date	**24/04/2012**	
Review Date	**23/05/2021**	
Protective Marking	**Official**	
Suitable For Publication – Freedom Of Information	**Yes.** (no restrictions – see section 9)	

Supporting Documents

Policy – directly supporting documents

- NPCC position on social media (Click here)
- Social Media Accounts: List of all available social media accounts. *(click here)*
- Twitter guidance *(click here)*

WMP policy reference documents

- Government Security Classifications (*Click here to download*)
- *Code of Ethics (Click here to download)*
- GDPR *(Click here)*
- Dignity at Work *(Click here)*
- West Midlands Police Disciplinary Policy (police staff) *(Click here)*
- Standards of Professional Behaviour Policy (*Click here*)

External reference documents

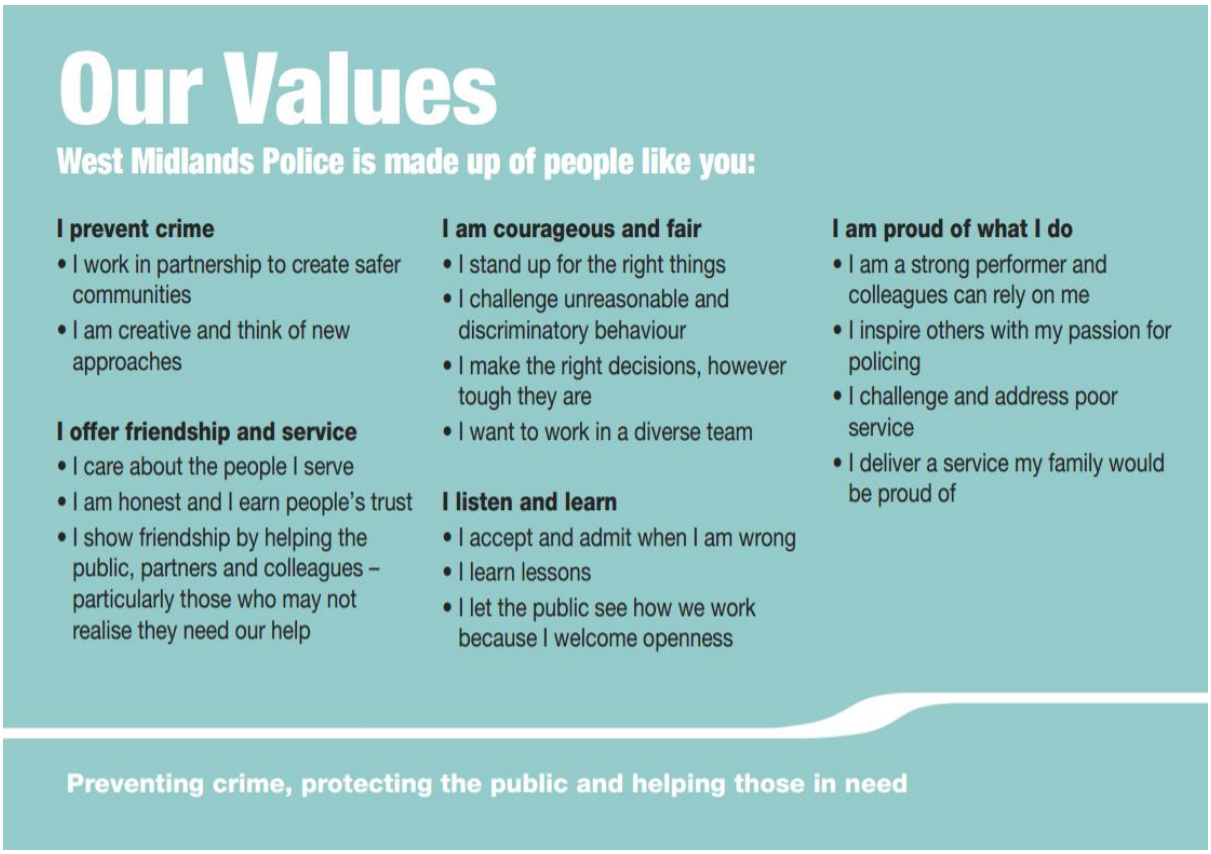
- Freedom of Information *(click here)*
- The Police (Conduct) Regulations 2012 *(Click here)*

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Values



Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing. (See supporting documents).

Alongside the Code of Ethics, The Standards of Professional Behaviour reflect the expectations that the police service and the public have of how police staff should behave. (See supporting documents).

The policy contained in this document seeks to build upon the overarching principles within the Code and Standards of Professional Behaviour to further support people in the organisation to do the right thing.

CONTENTS

1. INTRODUCTION.

1.1 This policy outlines both the Force's corporate use and also that of its officers and staff private use of social networking sites. Internet postings and video sharing websites such as Twitter, Facebook, YouTube and blogs. All references to personal accounts relates to personal officer accounts. All references to private use of social media relates to officers and staff private use of social media. This policy replaces Policy CC/01 version 1.5 with immediate effect, which is now withdrawn.

1.2 This policy should be read in conjunction with the series of guidance documents which are available on the Corporate Communications Department intranet here.

2. BACKGROUND.

2.1 West Midlands Police encourages officers and staff throughout the organisation to use social media as part of day to day business to engage the public and develop stronger community trust and confidence.

2.2 The use of digital and social media has an increasingly important impact on all areas of policing, from local policing to public order, investigation to major incidents. The impact is specifically around engagement, transparency, accountability, intelligence and investigations. The importance continues to grow with the evolving policing landscape around democratic accountability, increased public involvement in policing and the changes in society which are seeing increased numbers of people using online services in all aspects of their lives.

2.3 The police service already has a broad tradition of community engagement which recognises the need for responsiveness, visibility and accountability. West Midlands Police recognises that traditional methods of communicating messages which have been relied on in the past are having less impact and are reaching fewer people. Therefore there is a real need to embrace other growing forms of communication.

2.4 Easy access to technology, broadband connections and mobile internet mean an online presence is part of everyday life. West Midlands Police has embraced this new form of communication as part of our strategy to engage the public, ensuring we evolve and develop our methods in line with those used by the public.

3. CORPORATE USE OF SOCIAL NETWORKING & VIDEO SHARING SITES.

3.1 The purpose of West Midlands Police corporate social media accounts is to:

- Be the first place for the public to find important information and news about West Midlands Police
- Increase trust and confidence
- Engage with the communities of the West Midlands about crime and anti-social behaviour
- Provide a feedback forum for the public to comment and engage with the force
- Publicise news, appeals and crime prevention information to assist investigations
- Publicise the work of all teams

3.2 All applications for new corporate accounts must be approved by the Corporate Communications Department before they are opened. West Midlands Police will own all accounts created by CCD as well as accounts that are converted from a personal use to a policing use. CCD do not own accounts managed by staff networks – these fall under staff network's social media policy.

3.3 Individuals and teams can apply for a social media account that will be considered on a case by case basis.

3.4 Any officer or staff member who wishes to open a corporate account must get approval from their line manager, and demonstrate that the account will fulfil the following criteria:

- That it has a policing purpose
- That they understand their responsibilities in managing the account (highlighted later in this document)
- They have familiarised themselves with guidance on the intranet (click here)
- Agree to all the elements of this policy

NB. The application form can be found on the intranet here

All applications must be submitted in an email to socialmedia@west-midlands.pnn.police.uk.

3.5 The Corporate Communications Department reserves the right to refuse new social media accounts, or close any social media accounts that do not comply with this policy.

3.6 Line managers must support applications for accounts and will be responsible for monitoring and supervising the content of the account, which must be in line with WMP Vision & Values.

3.7 All social media accounts must have their usernames and passwords registered with the Corporate Communications Department to ensure that corporate accounts can be protected and recovered.

3.8 Officers must also inform the Corporate Communications Department when they change their password, name of account, Twitter handle, bio or owner of the account at the time of its change.

3.10 Officers and staff registering corporate social media accounts must use their West Midlands Police email address for the account.

3.11 The primary West Midlands Police social networking sites (i.e. Force Facebook/Twitter/Instagram/YouTube and Snapchat) will be administered by the Corporate Communications Department.

3.12 Social media should always be considered as one channel for communication, and should not be used in isolation. Notify CCD immediately if you have posted something that is going to attract media attention regardless if it's good or bad.

3.13 Apps such as Hootsuite are added to accounts by Corporate Communications and must not be deleted by users.

3.14 For security reasons, social media users should not give any third party apps access to their accounts.

3.15 Location services on social networks should be turned off at all times to protect operational security.

3.16 Private and Instant messenger tools within social media applications will not be used to send evidence and policing material. This includes Whatsapp, Facebook Messenger and emails on personal devices.

Social media, private and instant managing tools will not be used to send personal information relating to any caller, victim, witness, suspect or colleague and any other individual whose personal details we hold, unless it serves a policing purpose.

Cases at court can be placed in jeopardy if pertinent communications are made over private messenger or direct message on personal phones.

You may be liable to personal prosecution under the Data Protection Act 2018 or Computer Misuse Act if you obtain or disclose personal information unlawfully. As a result your personal device maybe taken off you and treated as evidence.

4. MANAGEMENT OF CONTENT.

4.1 All social networking output must be accurate, up to date and relevant, with a regular flow of new content to maintain user interest.
Out-of-date content such as an appeal should be removed as soon as it becomes out of date. Monthly reviews should be conducted to delete anything that is out of date or subject to ongoing legal proceedings. For this reason social media users are advised NOT to do their own wanted appeals or missing person's appeals.

4.2 The development of the Force's corporate sites will be the responsibility of the Corporate Communications Department. Account owners will be responsible for the content of local sites. Line supervisors will be responsible for monitoring the accuracy and relevance of local content. Relevant senior leadership teams are responsible for the overall governance of local content under the direction of the Corporate Communications Department.

4.3 The Corporate Communications Department will have access to all sites and will remove inappropriate material without notice.

4.4 As with any force system, the force retains the right to access all corporate social media accounts, including private and direct messages, to ensure that they comply with the law and force policies, and will issue guidance to officers where appropriate. Information may be shared with relevant parties where appropriate. Direct messages

should be considered public information which is obtainable under Freedom of Information requests.

4.5 Any serious complaints, issues, discrepancies or breach of this policy or accompanying guidance with any force accounts will be dealt with in the first instance by the Director of Corporate Communications. PSD, local command teams or departmental heads or above will be informed if necessary. Those decisions will be made on a case by cases basis.

4.6 All video footage, comments, text and photographs appearing on social networking sites should reflect the corporate nature of the site. Nothing should be posted that could bring the Force into disrepute or conflict with our corporate message/style.

4.7 Any information, messages, comments, pictures or video footage which is posted should serve a clear policing purpose. Every opportunity should be used to promote force key messages around reassurance and keeping people safe.

4.8 Messages about major incidents, missing or wanted people, must only be posted from the main WMP / NPU accounts.
Full responsibility for social media messages about these incidents remains with the SIO and Corporate Communications Department, although they can be retweeted from any account. Training will be provided by CCD.

4.9 No sensitive information should be posted on social media (see GSC above for clarification).

4.10 It is the responsibility of the NPU or department posting photographs or footage to ensure that they comply with legal or data protection requirements and, if necessary, a risk assessment and/or EQIA should be carried out. Photographs and footage that could compromise an operation or jeopardise a court case must not be posted, nor photographs that sensationalise incidents, such as pictures from serious road traffic collisions. Before posting or uploading any footage or photograph, you should carefully check it so that innocent bystanders are not identifiable. If you choose to use a photograph make sure you have complied with the data protection law and if applicable, obtain consent. If you have any queries about posting you should speak with the Corporate Communications Department.

4.11 Any appeals for wanted or missing people should link to the relevant page on the force website or Flickr so that images can be removed promptly and effectively once people are found. NPUs and departments should not post their own appeals for wanted or missing people without agreement from Corporate Communications Department and a communication strategy.

4.12 Uploading any information to social networking sites is a form of disclosure and therefore must comply with data protection principles. Officers and staff should also ensure that they are familiar with the Freedom of Information Act 2000 & GDPR (See supporting documents).

4.13 Images that are not owned by yourself or WMP must not be used for example using images from Google could infringe copyright legislation however Twitter Gifs and images provided by Twitter are acceptable.

4.14 Where possible, links back to the main Force website (www.west-midlands.police.uk) should be used to help provide context and background as well as to help drive traffic onto the main site.

4.15 All social media bios will clearly display an agreed disclaimer. This can be obtained from the Corporate Communications Department and directs people on how to report a crime and contact police.

4.16 In the event of a major incident or an emergency, follow official force channels for instructions and do not issue any messaging to the public without prior authority from Corporate Communications.

4.17 Refer to Relationships with the Media policy, if you are approached by a journalist via social media.

4.18 Any police officer or staff member who no longer wants to have an official account must either pass the account to another team member to carry on (informing the Corporate Communications Department when this happens) or close the account down. If an account is closed the owner must inform Corporate Communications.

4.19 Anyone who wishes to change an official account to a personal account should consult Corporate Communications. Anyone who wants to post in an official capacity on a personal account should consult Corporate Communications.

4.20 Users should not use live video broadcasting platforms such as Periscope, Facebook Live, etc, without prior agreement from the Corporate Communications Department.

4.21 Use of WM Now is covered by its own policy, but many of the above also apply to it.

4.22 Users must be conscious that whatever they put out on social media can potentially be seen by millions of people and is often picked up by journalists.

4.23 Be aware of other information in the public domain. Be aware that other users could identify the subject of your tweet even if it does not contain any names/locations.

4.24 In line with national and force policy, officers are reminded that social media messaging in connection with any incident or investigation may need to be disclosed at a later date. Officers posting text, pictures or video on social media relating to any incident or investigation have a duty to update relevant logs with a message to say they have done so.
If there is not an open log, officers have a duty to notify the OIC of the existence of the social media message. If there is any doubt about what does or does not need to be recorded, guidance will be available from supervisors.

4.25 We want officers to proactively talk about success, but they need to consider the evidential and potential disclosure impact of sharing before you do so.
If what you are sharing is something that might have an evidential impact on the case, consider if it is the right thing to do at that point.
For example, are you sharing a picture of an item that has been recovered before a S18 search has been carried out?
Similarly, will disclosing the fact that an item such as a firearm has been recovered potentially put someone at risk?

Removal of Content:

4.26 It is the post author's responsibility to publish content that is accurate, up-to-date and factually correct.

4.27 If a request is received from the member of the public to remove or amend inaccurate or out–of-date personal information on social media, the request should be referred to

Information Security & Assurance as soon as possible - information_security@west-midlands.pnn.police.uk

4.28 Requests can be made in writing or verbally – the internal process for each is the same. Information Security & Assurance will liaise with the relevant teams to verify the request, will make the decision as to what action should be taken, will coordinate any rectification / erasure, and will respond to the member of the public accordingly.

4.29 Any content containing inaccurate or out-of-date information will be removed by a member of the social media team.

4.30 If the information is not removed, the member of the public will be informed and told the reason/s why. Communications with the member of the public will include a notification of their right to make a complaint to the Information Commissioner's Office, or to seek to enforce this right through judicial remedy.

4.31 The Data Protection Act 2018 and the GDPR require that requests are responded to without undue delay, and in any case within one month, however this can be extended to three months for particularly complex cases if the reason is explained to the data member of the public. In order to ensure we are providing a satisfactory service to the public, and to ensure we operate within the statutory time frames, the request should be considered and any removal completed within a maximum of 14 days.

5. PERSONAL AND CORPORATE ACCOUNT SECURITY.

5.1 Due to potential risks to the security of the user, and that of their family and their friends, all officers and staff should be aware of the need to protect themselves and their personal information online whilst using all personal social media accounts.

5.2 Ensure that your security settings on personal social media accounts are set to the maximum for your own safety. More Information from Facebook is available here.

5.3 When posting information on social media sites, both personal and corporate, consider the risks:

- Personal safety and exploitation of personal information. Avoid providing addresses phone numbers, email addresses etc.
- The security of the organisation
- Security of information relating to family, friends and other contacts
- Referencing your role or the organisation
- If you are using a mobile device, consider turning off any GPS/location tracking options within social media apps that identify your location.

5.4 Officers and staff should not make reference to West Midlands Police on personal social media accounts, particularly if comments are critical, or ridicule the organisation or other colleagues. Please refer to Dignity at Work policy for further guidance. (See supporting documents).

5.5 Whilst it is acknowledged by the Force that officers and staff may choose to use their own personal mobile phones to update their corporate social media accounts, users are reminded to be careful about the security of their own equipment. If a personal mobile device with a police social network is lost, the officer or member of staff must contact the Corporate Communications Department as soon as possible.

5.6 Any lost phones or computers with West Midlands Police social media accounts should be reported to Corporate Communications so that the account can be protected.

5.7 The administrator of any social media account is responsible for the management of the account's password. The administrator should observe appropriate security levels in relation to these shared account passwords. Administrators should keep details of all staff members with access, and change passwords when team membership changes.

5.8 Be careful about adding applications to social media accounts as you will often be granting permission to access account information to a third party provider and therefore may compromise the security of your account

5.9 Change passwords regularly, but always share it with CCD.

5.10 When using personal corporate account please users should not express personal views which may be controversial, derogatory towards colleagues or West Midlands Police, or conflict with organisational views on police social media pages. Refrain from expressing political opinion on Force accounts. Do not post inappropriate comments, share or like inappropriate or offensive material which will associate your account with controversial and derogatory subjects.

6. PRIVATE USE OF SOCIAL NETWORKING & VIDEO SHARING SITES.

6.1 Prior to joining West Midlands Police, we advise a full review of your social media accounts to make sure no historical content exists which could breach this policy.

6.2 All staff are accountable for whatever they send on social media in both a public and private capacity. This includes direct messenger services and private messenger tools.

Inappropriate use, harassment, bullying or disclosure of personal information about other individuals, colleagues, victims, offenders, suspects or witnesses and the force on social networking and video sharing sites, or private messaging tools including Facebook Messenger, Whatsapp, or any other form of direct messenger is subject to criminal and/or misconduct procedures.

You may be liable to personal prosecution under the Data Protection Act 2018 or Computer Misuse Act if you obtain or disclose personal information unlawfully.

6.3 When identifying yourself as an employee of West Midlands Police on social media, bear in mind your personal and operational security at all times.

6.4 Users should also be aware that the media use social media to gather information about officers and staff, including personal details, telephone numbers, e-mail addresses and links, images and interests, and are entitled to report on anything posted.

6.5 All officers and staff must note that any comments made on social media will be deemed to be in the public domain and seen as official police comment. Any comments could therefore be liable to a misconduct severity assessment under the Force's Disciplinary Policy (Police Staff) or the Police (Conduct) Regulations 2012 for Police Officers (see supporting documents). This applies to both personal and corporate sites.

6.6 To protect the reputation of the Force and its individuals, officers and staff, users should not express personal views which may be controversial, derogatory towards colleagues or West Midlands Police, or conflict with organisational views on their personal social media pages. Refrain from expressing political opinion on private accounts which are controversial. Do not post inappropriate comments, share or like

inappropriate or offensive material which will associate your account with controversial and derogatory subjects.

6.7 Comments made on personal sites should not reveal confidential information or jeopardise operational matters.

6.8 When using private social networking, blogs and video sharing websites, no use may be made of the West Midlands Police name, crest or insignia without the express permission of the Corporate Communications Department. Consideration must also be given to any other matters of copyright.

6.9 When using private networking no use may be made of force photographs or images without the permission of the Corporate Communications Department.

6.10 No police officer or staff should send messages about West Midlands Police work, operations and activity from personal / non-corporate social media accounts.

6.11 To protect the reputation of the Force, as well as protecting the reputation of its police employees, officers and staff should not set up unofficial or spoof police groups, pages or accounts.

6.12 During election periods, be mindful of sharing any content that could be perceived as showing a political allegiance.

6.13 Personal and corporate social networks should not be used to establish or pursue a sexual or improper emotional relationship with any current or former victim, offender or witness, or use any social media accounts to pursue a relationship with someone close to these groups.

6.14 If officers or staff are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

6.15 Breach of this policy may result in misconduct proceedings. Dependent on the case it could result in dismissal. Any officer or staff member suspected of committing a breach of this policy will be required to co-operate with our investigation. All cases will be looked at on a case by case basis.

6.16 Users may be required to remove any social media content that the Force considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

6.17 If you see any inappropriate comments or have any concerns about cyberbullying and harassment, they should be reported in line with the data protection policy and dignity at work policy. (See supporting documents).

7. EQUALITY IMPACT ASSESSMENT (EQIA).

7.1 The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how WMP has evidenced ‘due regard’ to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.

- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

8. HUMAN RIGHTS.

8.1 This policy has been implemented and reviewed in accordance with that set out with the European Convention and principles provided by the Human Rights Acts Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm, affecting that of:

- Right to respect for private and family life *(Article 8 – section 2):*
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Appeals for missing persons and those wanted in association with crimes within the West Midlands would be included in the above article.

9. FREEDOM OF INFORMATION (FOI).

9.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 2.1 of this policy has been GSC marked as Official and is fully disclosable to members of the public via the Force WMP internet website.

9.2 Public disclosure does not automatically apply to supporting Force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
No issues version 2.1	n/a	n/a

10. TRAINING.

10.1 CCD is trained to provide on-going advice and technical support to all officers and staff with regards to social media.

10.2 Guidance on getting the best out of social media is available here.

11. PROMOTION / DISTRIBUTION & MARKETING.

11.1 The following methods will be adopted to ensure full knowledge of the Policy:

- Policy document and associated documents on the Force Intranet (noticeboard) for the attention of all WMP officers and staff;
- Recording and audit entry in the Force policy library & publication on the Force Policy Portal
- Intranet marketing via Corporate Communications Department – Social Media team.

12. REVIEW.

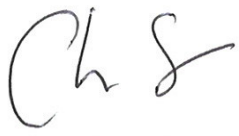
12.1 The policy business owner Corporate Communications maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

12.2 The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

12.3 A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted by the date shown as indicated on the first page.

12.4 Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

12.5 Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.



CHIEF CONSTABLE

13. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.0	24/04/2012	New Force policy. (supersedes Order 34/2009).	New Force policy approved by CC Sims.
1.1	27/04/2012	Removal of sub-section 6.7 and grammar change to 6.6	James Mullins – Force information Security Manager and David Hodgetts – Communications Manager.
1.2	20/08/2012	Changes and additions to sections 2.1, 3.4, 3.8, 4.4, 4.8, 5.1, 5.2, 5.8, 6.4, 6.5, 6.8, 6.17, 6.18, 6.20	Amended by David Hodgetts, agreed with Dan Barton – Head of Corporate Communications – and approved by DCC Thompson
1.3	04.10.12	Minor grammatical changes	PS 4566 Brookes
1.4	20.03.14	Minor amendments and additions, plus re-formatting so put corporate use first and personal use last.	Amended by David Hodgetts, agreed with Dan Barton – Head of Corporate Communications and Ch Insp Deb Doyle, PSD
1.5	01/12/2015	Minor Changes/additions to sections: 3.3, 3.13, 3.14, 4.5, 4.8, 4.12, 4.14, 4.24, 5.6	Jackie Harrison, Pete Edney
2.0	05/07/2018	New supporting documents linked to New policy reference documents linked to, including GDPR and Dignity at Work, Disciplinary at Work (Police Staff), and Police Conduct legislation (2012), Standard of Professional behaviour. P3 – Force values added and new policies in supporting documents. 1.1 Updated to reflect latest version numbers. Definition of personal and private added. 2.4 Tweaked wording 3.1 – Updated purposes of force social media accounts 3.2 – Updated statement on WMP ownership of force social media. Clarification over staff networks usage, accounts and private accounts which are converted to policing accounts 3.3 – Removed reference to WordPress and updated rules around which accounts will be considered. 3.4 – Clarification that anyone wanting a social media account must agree to all aspects of this policy. Contact e-mail address also updated. 3.6 – Clarified wording and added reference to WMP Vision & Values	Mike Woods/Hannah Fitzgerald/Asim Janjua

		3.8 (3.9 on previous version of policy) – Updated circumstances in which CCD must be alerted of changes to accounts/profiles. 3.11 – Clarified wording around CCD management of main accounts 3.12 – New requirement to alert CCD of messages which may attract media attention 3.13/14 – Clarified wording 3.15 – Instructions on location services 3.16 – New guidance around using personal, instant, direct messaging tools. Clarification about devices being seized. 4.1 - New guidance on management of content 4.3 – Clarified wording 4.4 – Clarified wording 4.5 – Updated details on handling of breaches of policy Process Clarified 4.8 – Updated guidance on messages around police incidents 4.9 – Updated security guidance 4.10 – Changed LPU to NPU, and added more guidance around images 4.11 - Updated position on appeals (merged with 4.12 from version 1.5) 4.13 – 4.23 -onwards - Significant changes to numbering scheme and content 4.26 – New guidance on removal of content following requests from the public, and processes for dealing with complaints 5.3 Wording changed 5.4 Dignity at Work policy added 5.9 – Reminder to change passwords regularly, but to always share with CCD 6.1 – New point about checking previous conduct 6.2 – Reworded and clarified. Additional points about instant messaging conduct. 6.4 Wording changed, policy added. 6.6 – Clarification over expressing personal/political opinion 6.13 – 6.15 – New sections 6.11 – Condensed wording 6.15 – Clarified dismissal process. 6.16 – New point created 9.2 – Updated version number 10 – Updated training information 12 – Updated sign off from current chief constable	

2.01	23/05/2019	4.24-4.25 – New guidance on disclosure issues	