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 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 1.5**	**01/12/2015**
Business Area Owner	**Corporate Communications Department**	
Department Responsible	**Corporate Communications Department**	
Policy Contact	**David Hodgetts - Communications Manager**	
Policy Author	**David Hodgetts - Communications Manager**	
Approved By	**Mr D. Thompson – Deputy Chief Constable**	
Policy Initial Implementation Date	**24/04/2012**	
Review Date	**01/12/2016**	
Protective Marking	**Not protectively marked**	
Suitable For Publication – Freedom Of Information	**Yes.** (no restrictions – see section 9)	

Supporting Documents

Policy – directly supporting documents

- Engage document – Assist police officers and staff in using technology when engaging with their communities *(click here)*
- Social Media Accounts: List of all available social media accounts. *(click here)*
- Twitter guidance *(click here)*

WMP policy reference documents

- Government Protective Marking Scheme (GPMS) *(click here)*
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*

External reference documents

- Data Protection Act 1988 *(click here)*
- Freedom of Information *(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 Diversity Vision Statement and Values

“Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values”

“All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay.”

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.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code 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 personal use of social networking and video sharing websites such as Twitter, Facebook, YouTube and blogs, and with immediate effect replaces Policy CC/01 version 1.3 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 site (HQ Departments > Corporate Communications > Social media).

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, inexpensive 'always on' broadband connections and the growing use of mobile internet access means that 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 are to:

- Be the first place for the public to find important information about West Midlands Police
- Increase trust and confidence
- Consult and inform the communities of the West Midlands of crime and anti-social behaviour
- Provide a feedback forum for the public to comment about policing in the West Midlands
- Publicise news, appeals and crime prevention information.
- Publicise the work of neighbourhood teams
- Promote West Midlands Police in a less formal and more approachable way

3.2 All applications for new corporate accounts must be approved by the Corporate Communications Department before they are opened.

3.3 Individuals and teams can apply for Twitter or Wordpress blog accounts. Individual and team Facebook accounts will not be considered.

3.4 Any officer or staff member who wishes to open an account must demonstrate that the account will fulfil the above criteria; that it has a policing purpose; that they understand their responsibilities in managing the account (highlighted throughout this document) and they have familiarised themselves with the appropriate guidance document owned by Corporate Communications.

NB. The application form can be found on the intranet here: http://intranet2/hq_departments/corporate_communications/social_media.aspx.

All applications must be submitted in an email to corporate_communications.

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 Before any social media account is established, officers must have approval from their line manager, and must be able to show a clear policing purpose and demonstrate the business benefits linked to the Policing Plan.

3.7 Line managers will be responsible for monitoring and supervising the content of the account.

3.8 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 if hacked.

3.9 Officers must also inform the Corporate Communications Department when they change their password, name of account 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 All West Midlands Police corporate social networking and video sharing sites 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.

3.13 All corporate accounts must agree to accept Hootsuite or any other third party apps used by West Midlands Police Corporate Communications Department. Any apps added to accounts by Corporate Communications must not be deleted.

3.14 Social media users should not give any third party apps access to their accounts in order to keep the accounts as secure as possible

4. MANAGEMENT OF CONTENT.

4.1 All social networking, blogs and video sharing sites must be accurate, as well as kept up to date and relevant, with a regular flow of new content to maintain user interest. Out-of-date content should be removed as soon as it becomes out of date.

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 be capable of removing inappropriate material. Therefore login account details must be forwarded to the Corporate Communications Department, who will maintain a list of all accounts. Changes to login details and passwords should be notified to the Corporate Communications Department. Any applications added to social media accounts by Corporate Communications must not be deleted.

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 policy and guidelines, and will issue guidance to officers where appropriate. Direct messages should be considered public information.

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 Head of Corporate Communications, local command teams or departmental heads and ultimately the Deputy Chief Constable if necessary.

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 incidents managed by Force CID, Public Protection Unit or other live major incidents must only be tweeted in conjunction with the Corporate Communications Department. Full responsibility for social media messages about these incidents remains with the SIO and Corporate Communications Department, so officers should only re-tweet / copy messages from the main Force or LPU accounts.

4.9 No information that would be considered Restricted/Official or above should be posted on the site (see GPMS).

4.10 It is the responsibility of the LPU 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 road traffic collisions.

4.11 Photographs of offenders, victims and missing people should not be sent from officer and staff social media accounts. These images can be sent by Corporate Communications following normal procedures for issuing pictures, which can then be re-tweeted by other accounts.

4.12 Any appeals for wanted or missing people should link to the main website www.west-midlands.police.uk or WMP Flickr site so that images can be removed promptly and effectively once people are found. LPUs and departments should not post their own appeals for wanted or missing people without agreement from Corporate Communications Department and a communication strategy.

4.13 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 (See supporting documents).

4.14 Photographs of wanted people, including custody photos and CCTV appeals, should only be posted directly onto local social networking with agreement from Corporate Communications first. Links to the main Force website or WMP Flickr site should be used to preserve the control and copyright of these images.

4.15 The social media sites must not be used for any kind of surveillance or monitoring work, such as tracking the activity of offenders, without the proper authority.

4.16 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.

4.17 All pages 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.

4.18 Official social media users must follow the guidance laid out in the relevant social media guidance document. This is available on the Corporate Communications Department intranet site.

4.19 The Corporate Communications Department will send messages to social media users with directions or instructions. These should be followed by all social media users.

4.20 Social media accounts should not be used to liaise with journalists. All requests from journalists or information to be given out to journalists should be coordinated by the Corporate Communications Department.

4.21 WMP users should not share any information about incidents directly with local blogs, Twitter accounts, or Facebook pages. The release of information should be managed by Corporate Communications.

4.22 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.

4.23 Nobody can change an official account to a personal account and nobody should change a personal account into a corporate account.

4.24 Twitter users should not use live video broadcasting platforms such as Periscope, Blab and Meerkat without prior agreement from the Corporate Communications Department.

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 social media accounts are set to the maximum for personal safety.

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
- Indirect reference to 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.

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 should 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 account information to the third party provider, and therefore may compromise the security of your account.

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

6.1 All staff are accountable for whatever they put into the public domain even in a privately held account. Inappropriate use or inappropriate disclosure of personal information on social networking and video sharing sites is subject to criminal proceedings (in accordance with s55 of the Data Protection Act it is a criminal offence to disclose personal information unlawfully) and/or misconduct procedures.

6.2 Officers and staff can identify themselves as a police officer or member of police staff on personal social networks, but should not identify themselves as working for West Midlands Police. This includes posting pictures of themselves in uniform or identifying working locations.

6.3 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.

6.4 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. This applies to both personal and corporate sites.

6.5 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 police social media pages.

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

6.7 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.

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

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

6.10 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.

6.11 During election periods police officers and staff should not post comments which could be judged to express political opinion on their own social networking sites, or on other peoples sites (in particular the political candidates). This is particularly important during elections for Police and Crime Commissioners.

6.12 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.

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 1.5 of this policy has been GPMS marked as Not Protectively Marked 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 1.5	n/a	n/a

10. TRAINING.

10.1 The Social Media team c/o Corporate Communications Departments are trained to provide on-going advice and technological support to all officers and staff with regards to all corporate social media sites.

10.2 Supporting guidance has been produced as to all types of social media accounts, twitter, and use of 'engage' which sets out to assist all police officers and staff using technology when engaging with their communities.

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.

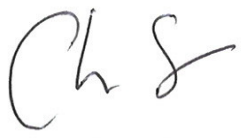
12.1 The policy business owner Corporate Communications maintain outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

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