



SOCIAL AND DIGITAL MEDIA POLICY

Executive Summary

This policy outlines how West Midlands Police (WMP) officers and staff will use social media and instant messaging to engage with communities and each other, to support the force strategy, objectives and priorities. It outlines how staff are expected to use social media, and the public's expectations of them on social media, and the support staff can expect from the Corporate Communications Department (CCD).

Authorised Professional Practice (APP)

This policy has been checked against APP. WMP have adopted the [Media Relations APP](#) with supplementary information contained herein.

Scope

The Chief Constable has overall direction and control of WMP and is ultimately accountable for all policies and supporting documents of the organisation and its actions. Adherence to this force policy will be expected from all employees and representatives of WMP.

Objectives

- **Ensure Professionalism in Online Engagement:**
 - Provide clear guidelines for officers and staff on how to conduct themselves online, maintaining professionalism and adhering to WMP's values and ethical standards.
 - Ensure that both corporate and personal social media accounts are used responsibly to uphold the reputation of WMP.
- **Support Communication with Communities:**
 - Enable WMP to engage effectively with the public via social media platforms to share information, raise awareness, and promote community participation in policing efforts.
 - Foster a two-way conversation between WMP and the communities it serves, helping build trust and transparency.
- **Align Social Media Use with WMP's Strategic Objectives:**
 - Ensure that social media content supports WMP's vision, strategic priorities, and objectives, helping the force achieve its goals in crime prevention, safety, and community outreach.
- **Protect Sensitive Information and Operational Integrity:**
 - Safeguard operational information and sensitive data, ensuring that social media use complies with legal standards, such as General Data Protection Regulation (GDPR), Data Protection regulations, and the Data Protection Act.
 - Prevent the sharing of sensitive police information (e.g., ongoing investigations, suspect details) that could undermine public trust, compromise investigations, or breach legal obligations.
- **Encourage Safe and Secure Use of Social Media and Instant Messaging:**
 - Provide staff with guidance on using personal and professional social media accounts safely, with special emphasis on privacy, security, and protecting personal data.
 - Set clear boundaries on the use of instant messaging apps to prevent misuse for sharing sensitive or operational police-related information.



- **Promote Consistency in Messaging:**
 - Ensure that content shared via corporate social media accounts is consistent, accurate, and aligned with WMP's broader communication strategy.
 - Guarantee that posts and updates are clear, relevant, and do not undermine operational or legal processes.
- **Maintain Public Trust and Transparency:**
 - Uphold the integrity of WMP by ensuring that public-facing communications are respectful, transparent, and demonstrate accountability.
 - Manage how WMP communicates sensitive topics (such as crime, incidents, or investigations) to the public in a manner that is responsible, accurate, and empathetic.
- **Provide Training and Support:**
 - Offer ongoing support and training to officers and staff to enhance their understanding of the appropriate use of social media and digital platforms.
 - Equip staff with the knowledge and tools needed to engage with communities effectively while adhering to force policies.
- **Ensure Accountability and Compliance:**
 - Establish clear procedures for monitoring and reviewing social media activity to ensure staff comply with the policy.
 - Outline the consequences of breaching the policy, ensuring staff understand their responsibilities and the potential disciplinary actions for non-compliance.

Definitions/Acronyms

APP	Authorised Professional Practice
BWV	Body Worn Video
CCD	Corporate Communications Department
DD	Digital Desk
GDPR	General Data Protection Regulation
IM	Instant Messaging
LPA	Local Policing Area
NPCC	National Police Chiefs Council
PIR	Police Intelligence Report
WMP	West Midlands Police

Policy Statements

1. INTRODUCTION

- Social media is a vital tool to:
 - Engage with communities
 - Raise awareness of developing issues and incidents
 - Encourage active citizenship and participation in our services
 - Allow a two-way conversation between WMP and the communities it serves.



- Social media channels used by the force will change over time, they currently include:
 - Facebook - <https://www.facebook.com/westmidlandspolice/>
 - X - <https://x.com/WMPolice>
 - Instagram - <https://www.instagram.com/westmidlandspolice/>
 - YouTube - <https://www.youtube.com/westmidlandspolice>
 - LinkedIn - <https://www.linkedin.com/company/3840/>
 - TikTok - <https://www.tiktok.com/@officialwmp>
 - Flickr - <https://www.flickr.com/photos/westmidlandspolice/>
 - Threads - <https://www.threads.net/@westmidlandspolice>
 - Snapchat - username is westmidspolice
- The conduct expected by officers and staff is aligned to the following policies and practices:
 - [Code of Ethics](#)
 - [Police Staff Council Handbook](#)
 - [GDPR and Data Protection Act](#)
 - [Dispute Resolution Policy](#)
 - [NPCC BWV Guidance](#)

2. TYPES OF SOCIAL MEDIA ACCOUNTS

CORPORATE	• Managed by Corporate Communications/LPA's or Teams/Departments/Force Executive Team/Supt/Chief Supt/Assistant Director • Branded with official imagery, logo, bio and website • Talk on behalf of West Midlands Police
PERSONAL	• Your personal social media – managed by you • Your account will not be branded as official WMP account • Standards of behaviour and legal compliance still apply to your personal accounts.

2.1 CORPORATE ACCOUNTS

- Corporate accounts are those created or authorised by CCD. They include WMP's branding, details of how to contact WMP and a link to the website.
- We have a clearly defined structure and hierarchy of social media accounts.
- The force uses the [REDACTED] platform to manage inbound messages from the public.
- Corporate accounts are created in line with national guidance, based on the needs of the public and the force.
- Applications for an account and to post messages on behalf of WMP will be limited to:
 - Corporate Communications Department
 - Superintendents and above
 - Assistant Directors
- If you fall outside the above listed categories and wish to post to social media as part of your role, CCD will assign a suitable Team or Department account for you to access.



- You must not create your own account which contains WMP branding and speak on behalf of the organisation without first consulting with Corporate Communications.
- Content on corporate accounts must support our vision, values, objectives, and priorities. CCD will set out what these are as part of initial inputs given to force social media users.
- Where practical, content and accounts must follow branding rules which are [outlined on the WMP Identity site](#).
- Anyone using social media in a professional capacity must do so:
 - with a clear policing purpose,
 - in line with our priorities and strategic objectives
 - in line with legislation covering criminal investigations, privacy, copyright and defamation.
 - With a clear understanding that sharing or otherwise amplifying messages from third parties will be seen as an endorsement and so must be avoided unless it is WMP or other partner messages that are being promoted.
- All posts must be accurate, up to date and relevant, with a regular flow of new content which meets our users' needs.
- Posts must never undermine operational, investigative, or criminal justice processes (for example, be in contempt of court).
- Body worn video must not be issued on social media unless Corporate Communications has been made aware and viewed the footage. BWV cannot be issued if it risks undermining an ongoing investigation, if a person has been charged or if there are sensitivities around the investigation.
- Basic operational information (name, date, location) of an incident is normally acceptable, unless it could jeopardise the investigation/a related investigation.
- Outdated content, such as an appeal which has served its purpose, must be removed as soon as possible.
- Monthly reviews must be conducted to remove content that is outdated or subject to ongoing legal proceedings.
- We reserve the right to monitor or record all communication on official social media accounts.
- Records of activity can be used by the organisation for quality assurance, conduct, discipline, performance, capability and/or criminal investigations.
- Any posts that attract inappropriate and offensive comments by the public will be removed by CCD or Digital Desk (DD). While many comments would fall into the category of unpleasant or unkind, others can cross the criminal threshold. It is vital that the force deals with any such messages (whether or not they cross the criminal threshold) and the impact they have swiftly and effectively. The force's Hate Crime Trigger Plan seeks to support colleagues, such as those CCD and those working on the DD, in taking appropriate action, while ensuring necessary support is in place for anyone directly affected by messages.



2.2 SHARING IMAGES OF KNIVES / BLADED WEAPONS

- Individual and team social media accounts must not share images of any knives/bladed weapons that have been recovered.
- Email images and details of the recovery/seizure to Corporate Communications, who will consider sharing images of knives/bladed weapons when there is a policing purpose.
- Corporate Communications will be the guardians of sharing all images of knives/bladed weapons so we can provide:
 - Context
 - Consistency
 - Appropriate style and tone
 - Share ways people can help/be active citizens in our fight against violence
 - Signpost to support agencies
 - Share with the appropriate key stakeholders
 - Links to our [Home - Life Or Knife - The choice is yours \(west-midlands.police.uk\)](https://www.west-midlands.police.uk/home-life-or-knife-the-choice-is-yours) website which has information on what we are doing to tackle knife crime, as well as toolkits for young people, parents and teachers

2.3 PERSONAL ACCOUNTS

- The [Code of Ethics](#), [Police Staff Council Handbook](#) and other regulations and restrictions on officers and staff apply to the personal use of social media.
- You must consider your safety, the organisational reputation and maintain the highest standards of behaviour both on and off duty, online and offline.
- Officers and staff are encouraged to review the privacy settings of their personal accounts to ensure they are secure
- If you are an officer or member of staff in a politically restricted role you must not use social media to play an active part in politics or share content which could interfere with the impartial discharge of your duties.
- Officers and staff who are not in politically restricted roles are free to express opinion online so long as it does not:
 - bring WMP's reputation into disrepute
 - break our Code of Ethics and Standards of Professional Behaviour
 - damage the relationship of trust and confidence between the police and the public
- You must consider your own safety and potential vulnerabilities if posting about your role and/or association to WMP.
- Anything posted in a personal capacity which is assessed as breaching the Code of Ethics and the [Police Staff Council Handbook](#) can be used in disciplinary proceedings if brought to the attention of the organisation.
- Users can post updates and insights about their roles but must take care never to undermine operational, investigative, or criminal justice processes (for example, be in contempt of court) with their updates.



- Personal account users must be aware that their content could be picked up by members of the public and media.
- Officers and staff must not show they work for the police for personal gain. This includes using photos of themselves in uniform on dating profiles.
- You must alert CCD in the event of media interest and be prepared to speak to CCD in the event of media interest coming into the press office.
- Any users of personal accounts must be aware that they may be seen by members of the public as representatives of the force and so the expected standards of behaviour must be upheld.

YOU CAN	YOU MUST NOT
✓ You can post about your day at work ✓ Talk in a professional capacity about your job, life in the police, insights ✓ Talk about your feelings/pride in the job ✓ Talk about your personal life – it's your personal account ✓ Share content from corporate accounts ✓ Signpost people to corporate accounts or formal contact methods	• Speak on behalf of WMP - You are not an official spokesperson for WMP • Have WMP branding (no logo, bio, website) • Post about specific jobs which identify location, people, policing tactics or is operationally sensitive. • Monitor performance • Gather reports/manage intel • Anything which brings WMP into disrepute or breaches Code of Ethics.
EXAMPLES	EXAMPLES
• "Had a great day at work, arrested two people, great work team" • "Really proud of the hard work me and my team did on this job [shares news story from corporate account]" • If anyone has any information, contact @WMPolice / West Midlands Police' • "I'm really sorry that's happened to you, please get in touch with WMP to discuss" (you could tag relevant account).	• "Arrested 2 people, 1 male, 1 female in custody on Smith Lane, Coventry". • "Really proud of the hard work me and my team did on this job [shares details of tactics, shares story themselves]." • "If anyone has any information get in touch with me and my team" • "I'm really sorry you're unhappy with the service. We're really stretched / Please get in touch directly"

3. INSTANT / DIRECT MESSAGING

- Instant messaging apps when used on personal devices, must not be used to communicate sensitive police information or operational policing matters under any circumstances (including but not limited to WhatsApp, Facebook Messenger, Instagram, X and Snapchat).
- This could constitute a breach of:
 - [GDPR and Data Protection Act](#)
 - [The Police Staff Council Handbook](#)
 - [Code of Ethics](#)
- Police information includes but is not limited to:
 - Details of ongoing investigations
 - Personal details of the public/victims/offenders/suspects/witnesses



- Evidential material
 - Data and information which must be recorded in police systems
 - Information and photos from the intranet/NewsBeat
- You can use instant messaging apps for informal discussions between colleagues, including arranging shifts or overtime at short notice.
 - You can use instant messaging apps to discuss work related matters so long as the content does not fall into the category of police information as described above or breaches the [Dispute Resolution policy](#).
 - Where possible other authorised force platforms and channels must be used. [REDACTED], which is being made available on all force devices, is a suitable alternative and allows for secure communication of material up to and including OFFICIAL SENSITIVE classification.
 - Information shared in [REDACTED] is subject to disclosure under [Freedom of Information](#) and other legislation.
 - During the annual integrity health checks which take place with your line managers you will be required to disclose membership of any WhatsApp groups used for any WMP work related purpose as detailed above. This information will be recorded on force systems.
 - Direct messaging must never be used to contact/engage with members of the public from personal devices.
 - Any attempt to contact a victim of crime, for a non-policing purpose:
 - will be considered as an abuse of position
 - may amount to a criminal offence
 - will be subject of investigation by the Professional Standards Department.
 - If you receive a direct message, tag or notification from a member of the public requesting information or advice, you must:
 - signpost them to a formal and auditable method of contact such as 999 for an emergency and 101, Live Chat, e-mail or appropriate WMP corporate social media account
 - request them not to send any further information via direct messaging.
 - inform supervision that the contact has taken place
 - Discriminatory or offensive content or content which breaches force policy e.g. [Sexual Harassment Policy](#) in private instant messaging conversations can leave you liable to face disciplinary proceedings.
 - You must be aware of the [Dispute Resolution Policy](#) and the expectations we have of your conduct when using private messaging tools.

4. INFORMATION SECURITY

- You must be aware of and adhere to Information Security Policies including:
 - [Information Security including all procedural guidance](#)
 - [Data Protection](#)
 - [Information Risk Management including all procedural guidance](#)



- Information placed on social media can be viewed by anyone - including those who may wish to do harm to you, your family, friends or colleagues.
- The responsibility rests with users that whatever is disclosed does not put anyone at risk.
- Do not share information from the Intranet/NewsBeat on social media unless shared publicly by WMP.
- More advice is available here: [Security for social media users](#)
- More advice is available on protecting yourself and WMP from malicious online profiles see [Home - Think Before You Link](#)

5. INTELLIGENCE

- If you become aware of intelligence circulating on social media that may not currently be known to WMP, you must create a PIR (if you have access to the system) or send it to [REDACTED]
- In the event that relevant information, such as a crime report, piece of intelligence or evidence, is passed to you on a personal account by a member of the public, it is the duty of the account holder to notify the force as soon as possible through the most appropriate channel.
- If a piece of content needs reporting to a social media platform, this can be done by the person who has viewed it. This is not the role of CCD or intel and you no longer need a social media account to do this.

6. CONCERNS AND COMPLAINTS

- If you believe content on either a corporate or personal account breaches this policy:
 - Attempt to secure and preserve any immediately available evidence
 - Bring the matter to the attention of your local Standards Manager for initial assessment and potential onward submission to the Professional Standards Department.
 - Any complaints or conduct that is reported must be brought to the attention of the local Standards Manager
 - The Standards Manager will secure immediately available evidence and if appropriate, forward onto the Professional Standards Department for consideration.

7. TRAINING

- CCD is responsible for training and advising social media users. If you feel you need or would like training you can contact CCD.

Relevant Legislation / Policies / Procedural Guidance

- [Media APP](#)
- [Code of Ethics](#)
- [The Police Staff Handbook](#)
- [GDPR and Data Protection Act](#)
- [Dispute Resolution Policy](#)
- [NPCC BWV Guidance](#)



- [WMP Identity Site](#)
- [Freedom of Information](#)
- [Information Security](#)
- [Information Risk Management](#)
- [Security for Social Media Users](#)
- <https://www.equalityhumanrights.com/human-rights/human-rights-act/article-10-freedom-expression>

Equality Impact Assessment

WMP places trust in their employees to comply with force policies and to work in accordance with and in support of:

[WMP Vision and Values](#)

[Code of Ethics | College of Policing](#)

[Voice of the Child](#)

	What impact has this policy had on the nine protected characteristics in relation to the three general duties? (If applicable)	How will this updated policy positively impact each of the nine protected characteristics in relation to the three general duties? If not, explain why it will not.
Age	Successful use of social media increases engagement. The various social media channels cater to a wide and varied age range rather than specifically targeting any particular age.	The engagement via social media platforms should increase as we are onboarding more platforms eg. Threads
Disability	The policy encourages users to follow brand, voice, and tone, which is designed to improve readability and accessibility.	No known effect on this protected characteristic.
Gender Reassignment	The policy did not reference the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages. Inappropriate and offensive comments can include details of protected characteristics.	The policy now references the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages.
Pregnancy & Maternity	No known effect on this protected characteristic.	No known effect on this protected characteristic.
Marriage & Civil Partnership	No known effect on this protected characteristic.	No known effect on this protected characteristic.
Race	The policy did not reference the Corporate Communications Department	The policy now references the Corporate Communications Department



	Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages. Inappropriate and offensive comments can include details of protected characteristics.	Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages.
Religion or Belief	The policy did not reference the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages. Inappropriate and offensive comments can include details of protected characteristics.	The policy now references the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages.
Sex	The policy did not reference the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages. Inappropriate and offensive comments can include details of protected characteristics.	The policy now references the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages.
Sexual Orientation	The policy did not reference the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages. Inappropriate and offensive comments can include details of protected characteristics.	The policy now references the Corporate Communications Department Hate Crime Trigger Plan which is our overview on what action needs to be taken where inappropriate and offensive comments are left on West Midlands Police's social media pages.

Publication Instructions

Suitable for publication to public.



Document Control

Strategic Lead: [role and name]	██████████ - Head of Corporate Communications
Policy Author(s): [role and name]	██████████ & ██████████ - News Managers
Effective Date:	26/05/25
FET Lead: [role and name]	ACC Welsted
Version Number:	1.6
Review Date:	26/05/27

Any enquiries in relation to this policy should be made directly with the Strategic Lead.

All policies are subject to a formal consultation process which encompasses Legal, Professional Standards, Faith Groups, Trade Unions, Independent Advisory Groups and wider force groups and any other relevant parties. A record of consultation can be found on the Policy Portal.

It is responsibility of the Strategic Lead to ensure that all links within the policy are correct and accessible.

Amendment History:

Version Number:	Effective Date:	Summary of Amendments:	Author:
1.1	13/07/2022	Following feedback from Trade Unions – minor amendments made to clarify wording in the policy	██████████ (TU)
1.2	08/11/2022	Clarified that NewsBeat/Intranet content should not be shared on social media, and added more security advice as well as advice on retweeting/amplifying messages	██████████
1.3	20/12/2022	Included section regarding sharing images of weapons	██████████
1.4	03/03/2023	Amended section on sharing images to specify as knives and bladed weapons	██████████
1.5	03/03/2025	Updated list of social media channels. Inclusion of BWV, Hate Crime Trigger Plan and Dispute Resolution Policy.	██████████ & ██████████
1.6	25/06/2025	Removal of Standards of Behaviour and replaced with The Police Staff Council Handbook including links	██████████