# SOCIAL & DIGITAL MEDIA

**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 – Media APP exists which covers issues such as the naming of suspects and disclosure obligations.

**Policy Statements:**

- 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
  - Twitter
  - Instagram
  - YouTube
  - LinkedIn
  - TikTok
  - Flickr

- The conduct expected by officers and staff is aligned to the following policies and practices:
  - Code of Ethics
  - Standards of Professional Behaviour
  - GDPR and Data Protection Act
  - Dignity at Work policy

## TYPES OF SOCIAL MEDIA ACCOUNTS

| | |
|---|---|
| **CORPORATE** | • Managed by Corporate Communications/NPUs or Teams/Departments/Force Executive Team/Chief Supt/Assistant Director<br>• Branded with official imagery, logo, bio and website<br>• Talk on behalf of West Midlands Police |
| **PERSONAL** | • Your personal social media – managed by you<br>• Your account will not be branded as official WMP account<br>• This policy will still apply to your personal accounts. |



West Midlands POLICE

## 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.
- 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 tweet on behalf of WMP will be limited to:
  - Corporate Communications Department
  - Force Executive Team (FET)
  - Chief Superintendents
  - Assistant Directors
- If you fall outside the above listed categories we 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.
- 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.
- 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).
- You can publish about operational information (name, date, location) of an incident.
- 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.

## PERSONAL ACCOUNTS

- The Code of Ethics, Standards of Professional Behaviour 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.
- 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 Standards of Professional Behaviour 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<br>✓ Talk in a professional capacity about your job, life in the police, insights<br>✓ Talk about your feelings/pride in the job<br>✓ Talk about your personal life – it's your personal account<br>✓ Share content from corporate accounts | • Speak on behalf of WMP - You are not an official spokesperson for WMP<br>• Have WMP branding (no logo, bio, website)<br>• Post about specific jobs which identify location, people, policing tactics or is operationally sensitive.<br>• Monitor performance |

| | |
|---|---|
| ✓ Signpost people to corporate accounts or formal contact methods | • Gather reports/manage intel<br>• 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"<br>• "Really proud of the hard work me and my team did on this job [shares news story from corporate account]"<br>• If anyone has any information, contact @WMPolice / West Midlands Police'<br>• "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".<br>• "Really proud of the hard work me and my team did on this job [shares details of tactics, shares story themselves]."<br>• "If anyone has any information get in touch with me and my team"<br>• "I'm really sorry you're unhappy with the service. We're really stretched / Please get in touch directly" |

## 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, Twitter and Snapchat)

- This could constitute a breach of:
  - GDPR and Data Protection Act
  - Standards of Professional Behaviour
  - 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

- 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 Dignity at Work policy.

- Where possible other authorised force platforms and channels must be used. Microsoft Teams, 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 Teams 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 Dignity at Work policy and the expectations we have of your conduct when using private messaging tools.

## 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.

- More advice is available here: Security for social media users

## 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 the FIB

- 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.

## CONCERNS & 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.

## TRAINING

- CCD is responsible for training and advising social media users. If you feel you need or would like training you can contact CCD.
- CCD have put together a training presentation 'Converting individual corporate accounts to personal'.

**Definitions/Acronyms:**

**IM – Instant messaging. Any tool that allows users to communicate privately with each other**
**CCD – Corporate Communications Department**
**WMP – West Midlands Police**

**Publication Instructions:**

- Suitable for publication to public

**Policy Ref: OTHER/4**

**Version: 1.1**

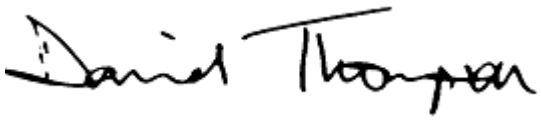
**Date: 13/07/2022**

**Review Date: 13/07/2023**

**Policy Author: Mike Woods**

***Any enquiries in relation to this policy should be made directly with the policy author shown above.***

**Force Executive Approval:**



**CHIEF CONSTABLE**



West Midlands POLICE

**Monitoring and Review**

| Version | Date Reviewed | No change / Minor Changes / Major Changes *(detail)* | Amended / Agreed by | New review date |
|---|---|---|---|---|
| 1.1 | 13/07/2022 | Following feedback from Trade Unions – minor amendments made to clarify wording in the policy | Asim Janjua<br>Mark Brittle (TU) | 13/07/2023 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |