



Social Media Policy



Contents

Overview	1
Rationale	3
Aim of the policy	3
General principles and accountability	4
Official social media accounts	5
Affiliated social media accounts	6
Standard protocol for official and affiliated users.....	7
Guidance, procedure and tactics.....	9
Personal social media accounts.....	9
Policy exemption	10
Procedural guides	11
Relevant legislation: (Human rights/diversity/Health & Safety/any other specifics)	11
Related references:	11
Identification, monitoring and review	12

Overview

This policy aims to ensure we have a contemporary, consistent and robust approach in line with our brand, Corporate Strategy, Police and Crime Plan and Policing Vision 2025. It has been developed by Communications and Engagement (C&E) following wide consultation with colleagues and research into other forces' social media policies.

The policy relates to all Gloucestershire Constabulary and OPCC employees, contractors and volunteers and is effective immediately. It recognises that there are three types of social media accounts associated with Gloucestershire Constabulary (GC) and the Office of the Police and Crime Commissioner (OPCC) and reflects the expectations for each of these. Due to their roles, the social media policy does not apply to the PCC's and Deputy PCC's accounts.

Please ensure that you are aware of the '[general principles and accountability](#)' of social media use before moving onto the three specific account types.

- [Official social media accounts](#)
- [Affiliated social media accounts](#)
- [Personal social media accounts](#)

To help you understand how each of these accounts differ and to help you identify which category you fall into – and which part of this policy applies to you - please refer to the below table. Please note that if you do not fall into any of these categories then please contact [Communications and Engagement](#) for more assistance.



Social Media Policy



	Official accounts:	Affiliated accounts:	Personal accounts:
Rationale for account	Official accounts are the voice of the organisation. This is where the public would first look to for information in the event of a crisis or concern.	Affiliated accounts are owned by individuals within the organisation who are of Chief Inspector ranking or above. Special consideration will be made for accounts that clearly serve a purpose that meets our expectations. They should be used to promote the work of the organisation as well as work within the account holder's policing roles.	Personal social media accounts are used outside of work to update your connections about your life, interests and activities.
Ownership	- These accounts are owned and monitored by C&E. They can be updated by C&E, or, devolved to no less than 2 local officers to update on behalf of the organisation. - C&E may also remove posts it feels reduce public confidence and could take over control of these accounts in a crisis.	- Individuals are owners of these accounts. They are monitored by C&E using the Force's social media management software. - Permission is required from C&E before accounts can be created. - C&E may remove posts it feels reduce public confidence and could take over control of accounts in a crisis.	You own these accounts and operate them outside of working hours
Content accounts are able to publish	Official accounts are the only accounts that can publish new organisational information such as operational activity and appeals in accordance to our guidance.	No new operational activity or appeals should be first promoted through these accounts. This should only take place through official accounts first. Posts can then be shared from the official accounts.	- Under no circumstances should you use the Constabulary or OPCC crests or official images. - Under no circumstances should you discuss operational activities or post information a member of the public cannot obtain publicly.
Guidance	Approval required where there may be a Press interest.	Personal messages can be posted but the account holder should be wary of media attention and comments which may attract criticism from the public.	You should avoid linking yourself to the Constabulary or OPCC in any online profiles; this includes professional development websites such as LinkedIn.
Visual presence and administration of account	The accounts must comply with the organisation's branding policy and be connected to our social media management software for monitoring and auditing purposes.	- A uniformed corporate photo should be used as the profile's photo. - C&E will be able to see all activity from these accounts and will monitor outgoing posts.	For security reasons, it is advised that you do not post any photos of you in uniform, it is also worth disassociating yourself from policing or the Constabulary.
Accountability	Training and guidance is always provided before a user can access an official account. If content breaches the guidance provided then more training will be offered. Users are accountable if a gross breach of behaviour.	The account holder is fully responsible for the content published on these account types C&E can provide support and guidance as and when required.	C&E monitors social media generally but does not actively monitor personal accounts. Any public posts on social media discovered by C&E that breach organisational policies will be forwarded to PSD to investigate.
Types of accounts	Our Facebook page @Glos_Police @ForestPolice	@SuptSmallwood @Robpriddy @andymorford350	- Personal Facebook profiles - Personal Twitter profiles
Next steps	Please read the following sections: General principles and accountability Official social media accounts Personal social media accounts	Please read the following sections: General principles and accountability Affiliated social media accounts Personal social media accounts	Please read the following sections: General principles and accountability Personal social media accounts



Social Media Policy



Rationale

Social & digital media is transforming the way society communicates. For us as a police force, it provides channels for more direct engagement with individuals, our communities, businesses and partner organisations. These engagement opportunities can help us to explain the diverse work we undertake on a daily basis and help to improve trust, satisfaction and confidence in us. It enables us to give advice and information, make appeals to help detect and tackle crime and to provide reassurance in times of a crisis. Gloucestershire Constabulary and the Office of the Police and Crime Commissioner (OPCC) recognise the opportunities and benefits associated with using these channels to engage and interact externally with a number of our communities. They can have a significant impact on the achievement of operational or corporate objectives, in particular community engagement. They have direct impact on our reputation as a Force and our relationships with staff, partners, service users and local communities.

This policy sets out the expectations of employees, contractors and volunteers who may use social media for **business use** and **personal use**. To help maintain our professional integrity and corporate reputation and help ensure we have safeguards in place, it is supplemented with guidance documents.

Aim of the policy

This policy is designed to provide support, structure and clarity for users of social media and digital media so you can operate within a safe, effective and appropriate manner. Social media, or social networking websites, are websites that enable users to share content and to interact with one another within a public forum. Examples of these websites are, (but not limited to); Facebook, Twitter, YouTube, Instagram, Snapchat, WhatsApp and blogs. Users must remember that these platforms should be used to enhance the reputation and integrity of the Constabulary and OPCC and be in line with our values: **integrity, impartiality, public service and transparency**.

A user is anyone who is employed either within a paid or voluntary capacity for the Constabulary or the OPCC. This includes all police officers (including Gloucestershire officers and staff working within a collaboration, such as Tri-Force and MCIT), police community support officers, special constables, Constabulary and OPCC police staff, contractors, volunteers, and approved users (including individuals on secondment to, or from, other forces) that are issued Constabulary or OPCC identification and system access.

All users must make yourselves aware of the following sections:

- [General principles and accountability](#)
- [Personal social media accounts](#)

If you use social media on behalf of the Constabulary or OPCC, you must make yourself aware of these sections:

- [Official social media accounts](#)



Social Media Policy



- [Affiliated social media accounts](#)
- [Standard protocol for official and affiliated users](#)

General principles and accountability

Gloucestershire Constabulary and the OPCC are professional, responsible and ethical organisations acting with honesty, integrity and humanity. These are expressed by our values (integrity, impartiality, public service and transparency). We expect people who work for us to adhere to our intent, values and principles, even in your personal time. There have been occasions where individuals have let down and discredited the work of the police service as a result of their behaviour and conduct on social media. One example where a police employee discredited their organisation made the national media and is featured below:



Clearly this is an inappropriate and insensitive message. This very public act weakens the confidence that the public have in the police - especially victims of this particular crime - and can undermine the hard work of other officers and staff.

There have been occasions within our own organisation where employees have sent inappropriate social media messages while on-duty or in their personal life. These cases have been investigated by the Constabulary's Professional Standards Department (PSD). Some of these cases have resulted in a misconduct proceeding.

Please remember that you are accountable for your social media use. Following the protocols set out below can help you to safeguard yourself, the Constabulary and OPCC from potential issues.

Things you mustn't do...

Make defamatory or other offensive comments on social media

It is worth remembering that social media is a public forum, even if your account is private, your followers can see your content. If people take offence to anything that you have done, they can screenshot this and share it within a public forum. The Code of Ethics is clear about how you should conduct yourself and this relates to social media too, even within your personal life.

If you make defamatory or offensive comments, it will be investigated by PSD. Communications and Engagement actively monitors all Official and Affiliated accounts. At times, activity on a



Social Media Policy



personal account has been brought to our attention and this has been forwarded to PSD for assessment and dealt with accordingly.

Posting political opinions on social media channels

Police officers must always remain apolitical and should not, either on a work or personal social media account, talk about political matters or share political views. This includes retweeting, sharing or liking messages of a political nature as this could be considered as endorsing an originator's views. The College of Policing's [Code of Ethics](#) clearly defines this matter.

It is commonly understood within social media that sharing, retweeting or liking of messages is often considered as an endorsement of an originator's views, even if you do so out of satire or in irony. To help you stay safe, this policy recommends that you always consider what you share, retweet or like.

What to do if you see inappropriate messages on any official, affiliated or personal social media accounts

If you have seen inappropriate content on any official or affiliated accounts, or on a colleague's personal account, you must report this to help minimise any risk or potential impact. The following reporting process is in place to enable you to provide information:

- **Report to your line manager**

Your line manager may be the best route to take to help with your concern. All line managers must deal with information provided in a sensitive and confidential way and pass it to PSD. If you are reporting a concern, a visual proof will help to provide context.

- **Report to PSD**

You are able to report concerns directly to PSD who will deal with them in a sensitive and confidential manner. PSD will investigate the report, so visual proof will help provide context.

- **Report anonymously**

If you feel that you would like to anonymously report any concerns, you can use the '[Anonymous contact system](#)' via the intranet. If you have visual proof, this will help to provide more context to the report.

Official social media accounts

Official social media accounts have been created to help the Constabulary and OPCC communicate and engage with our communities. With the exception of Chief Officer accounts, official accounts are maintained by teams within specific areas across the Constabulary all working towards a common purpose by offering:

- greater opportunity for transparency
- two way communication and better engagement
- assistance with operational matters
- communicating organisational information
- to build trust and confidence in the police.



Social Media Policy



Please refer to the [related references](#) section for more information about the principles and expectations for official accounts.

Using and accessing an official account

The following points form part of the social media policy and if you use an official account, they relate to you and you must adhere to them:

- Official accounts are created by C&E only and must not be setup by any individual or team.
- If there is a need for a new official account, requests must be made using the [social media request form found within the related references section](#) of this policy
- You must adhere to the [‘guidance’ and ‘Constabulary tone’ documents found within the related references section of this policy](#)
- If you are an existing user of an official account, you must access your accounts through C&E’s social media management software
- As a user, you have a paid licence with C&E’s social media management software, so it is your responsibility to inform C&E:
 - if you no longer require your login
 - if you move teams
 - if you are due to be on long-term leave
- If you are a new user and would like access to an official account, please email your request to communicationsandengagement@gloucestershire.pnn.police.uk for consideration
- Users of official accounts must adhere to the [‘standard protocol for official and affiliated users’](#) section of this policy
- Information about a crime or an incident can be proactively released to aid an investigation, with appeal points asking for the public’s assistance, to maintain public confidence in policing activity, or where it is a matter of public interest. Users should always consider the victim’s wishes when releasing information relevant to them.
- Appeal images will be removed from official account after 30 days. If the appeal is still live, the officer can ask for it to be publicised for a further 30 days by contacting the [External Communications](#) team.

Affiliated social media accounts

Affiliated social media accounts have been created to help senior members of the Constabulary to communicate and engage with our communities. Affiliated accounts are maintained by individuals within specific areas across the Constabulary and offer:

- an opportunity for transparency
- two way communication and engagement
- assistance with operational matters
- the opportunity to build trust and confidence in the police.

Please refer to the [related references](#) section for more information about the principles and expectations for affiliated accounts.



Social Media Policy



Using and accessing an affiliated account

The following points form part of this social media policy. If you use an affiliated account, you must adhere to these principles:

- Accounts must include these words in their bio: All views are my own and do not reflect those of my employer.
- Passwords must be eight characters long, include capitals and numbers and must be changed every three months.
- You must not display the Force crest within your profile or content.
- If you are an officer, you must include a uniformed photo as your profile photo. This can be your corporate photo or you may ask C&E for assistance in choosing an appropriate profile photo.
- You must consider the 'guidance' and 'Constabulary tone' documents found within the related references section of this policy
- You are responsible for responding to comments and direct messages.
- New affiliated accounts must be setup in conjunction with C&E and not created independently
- You can access your account through a browser or an app.
- Your account should not be the source of any appeals or operational matters as this is the responsibility of official accounts.
- Your account should look active. If it is dormant, please remove it.
- Do not post information about a crime or an incident not already shared by an official account. This should be done via the official accounts as the official source of information.
- You must adhere to the 'standard protocol for official and affiliated users' section of this policy.

Standard protocol for official and affiliated users

Publishing content, including posting images, videos

- Your social media activity must conform to principles set above either the 'principles for official accounts' or the 'principles for affiliated accounts' and the Code of Ethics. If it does not meet these, you must not post it.
- Do not publish images of the public, unless you have their permission. You might like to document all approvals within your officer pocket notebook.
- Do not publish images of children under the age of 18 without the signed consent of a parent or legal guardian. Please document all approvals within your officer pocket notebook.
- Do not publish an image of a Constabulary employee, unless you have consent from them. Please document all approvals within your officer pocket notebook.
- Do not publish CCTV images of unnamed suspects. All CCTV images in relation to a particular incident or crime must be directed to the Force Intelligence Bureau (FIB)¹ for it to distribute.
- Do not post any images of armed response officers or any other officer with guns unless approval is given by C&E
- Do not post any images or comments which show you consuming food or drink in a way that looks negative or makes it look like you are not working or being professional.

¹ The Constabulary adopts the national College of Policing's Guidance on the release of images of suspects and defendants



Social Media Policy



- It is your responsibility to ensure all content is appropriate and that there is no breach of copyright. You must adhere to copyright laws² when posting images or other online material.
- Do not publish photos that identify car registrations unless they are blurred/removed so it is unrecognisable.
- Do not publish photos that could identify a residential address or place of work especially in relation to a victim.
- Do not publish photos directly connected or related to a crime, incident, or an operation unless you have received specific approval from the OIC or SIO.
- Do not post any information about on-going criminal investigations or operations. This includes information which could undermine operational activity, including names or code names for exercises unless specific approval has been given by the OIC or SIO.
- If you want to share information about a crime or an incident that is newsworthy please let the External Communications team know details as soon as possible so they can deal with any subsequent media enquiries.
- Never post anything that could be considered rude, aggressive, sexist, racist or in any way that is likely to offend others.
- Do not post any disparaging or defamatory comments or statements about the Constabulary, colleagues, staff, residents, suppliers, partners and others.
- Do not post confidential information or information you only have access to via your role with the Constabulary. **Only non-official information should be shared and remember the Official Secrets Act.**
- Always consider the Government Security Classification (GSC) and the Data Protection Act when using social media, as you would when using other channels of communication.

Expectations of use

- You must engage with your followers and reply to messages publicly or privately.
- If an online conversation becomes problematic or is becoming negative then you should aim to move it offline so that it can be dealt with privately and limit any additional issues. This also helps minimise any criticism/embarrassment.
- During a major incident all access to accounts will be stopped to enable corporate messaging to be published in response to the incident.
- If you see anything that is offensive or illegal on any of our official or affiliated accounts, it is your responsibility to report it to C&E first, so that it can take down the post and report it to PSD for investigation.
- Contact C&E if you come across any social media content that disparages or reflects poorly on the Constabulary or OPCC, even if this is content that is not on a corporate channel, so that we can undertake a risk management review.
- If you see anything that is offensive or illegal on any other account then it is expected that you report this officially through to our Force Control Room.
- Do not create or participate in any discussions that are of a political nature or share any political views – tagging the central local, district, borough or county council account is

² Please visit: http://www.cla.co.uk/copyright_information/copyright_information for more information. If you would like to use images, video or any other media type ensure that it is free to use and free to redistribute. There is a search option for this within Google images.



Social Media Policy



acceptable, however individuals should not be tagged unless we are publically partnering with them for a specific event, occasion or campaign.

- Remember you are responsible for the accuracy of the information you post.
- Do not post personal views or opinions which criticise the values, policies or decisions of the Constabulary or OPCC.
- Do not post comments that might damage the reputation of Constabulary or OPCC or which could undermine public confidence in them.

Using social media for operational policing, covertly or for intelligence gathering

Any officer or member of Constabulary or OPCC staff must be aware of the Force guidance and the Regulation of Investigatory Powers Acts 2000 (RIPA) before gathering intelligence for an operational policing need using social media

Guidance, procedure and tactics

For guidance on how to use social media for an official or an affiliated account in a professional way and to conform to the expectations for them, please read the [guidance document in the 'related references' section at the bottom of this policy](#).

Personal social media accounts

As identified in the '[general principles and accountability](#)' section of this policy there is an expectation on how users must conduct themselves within their personal lives, please refer to this if you have entered straight to this section.

Users are fully accountable for the content that they create or share on their personal social or digital media accounts within the public domain, even on a privately held account and closed groups, including but not limited to, private Facebook groups or WhatsApp groups therefore the following principles apply:

- Do not include references to the Constabulary or OPCC within account names, or anything that might make you identifiable as an employee. This could include; images of you in uniform or any other identifiable clothing, collar numbers or call signs for example.
- Do not post any disparaging or defamatory statements about the Constabulary, colleagues, staff, victims or perpetrators
- Do not post confidential information or information you only have access to via your role within the Constabulary and remember the Official Secrets Act
- Do not talk about the Constabulary or the OPCC in a negative way or comment on anything work related that you find personally contentious. Raise any issues or concerns with your line manager, UNISON/POLFED representative or the Force's internal forum.
- Never display offensive images or make offensive comments, or in any way harass, intimidate, bully, victimise or discriminate against others.
- Do not post anything that may undermine the public's confidence in the Constabulary or OPCC or bring discredit to the Constabulary or OPCC either in or out of work time.



Social Media Policy



- Do not post or share anything that it is considered as privileged³ information such as Constabulary operations, projects, initiatives, change programmes, owned premises and personnel including your colleagues.
- Posts made on social or digital media will be deemed to be in the public domain and could be liable to a misconduct severity assessment.
- It is recommended that you do not post about the Constabulary or OPCC or your specific role within the respective organisation. If you do, this may impact on your own privacy, the security of family and friends. It may also compromise your vetting status or ability to be deployed on certain types of specialist policing
- The same risks apply, so please consider that if you indirectly refer to the Constabulary or OPCC people could make an informed guess and therefore this could leave you compromised. An example could be by sharing content from any Official or Affiliated account.
- If you disclose that you work for the Constabulary you should make it absolutely clear that any views expressed are yours alone and do not represent the official position of the Constabulary. However this does not prevent the Force from taking action if the policy is breached.
- Remember that social media is a public forum, the media and even criminals could access your personal accounts and are entitled to gather information about officers and staff, including personal details, telephone numbers, email addresses and links, images and interests.
- For more information on how to protect yourself on social media, please view the [social media guidance in the related references section](#).
- It is within the jurisdiction of Professional Standards Department (PSD) to investigate any reports of inappropriate social media use as explained above.

Policy exemption

Policy should enable consistent and effective decision making. Where operational or managerial circumstances require any decision-making that would adversely affect adherence to the policy or procedure. if an officer/police staff member believes that they need to make a decision that steps outside of policy and procedure they should do so, provided that:

- it is in line with the Constabulary's 'Statement of Intent' and the police service's 'Code of Ethics'
- the officer/police staff member:
 - raises the matter at the earliest opportunity (and ideally before any such decision is made) with their line manager declaring their intended (or actual) course of action if notification is made after the decision is taken
 - produces, in a timely manner, a signed and dated written explanation of why it is/was deemed necessary to step outside of policy and procedure, and
 - maintains an adequate record of this written rationale for audit purposes appropriate to the circumstances/contravention.

• ³Privileged information is information that a normal general member of the public would not have access to and is information that is acquired as a result for working for the Constabulary or OPCC.



Social Media Policy



Procedural guides

Relevant Legislation: (*Human rights/diversity/Health & Safety/any other specifics*)

Related References:

Principles and expectations for official accounts

Official accounts are considered as corporate communication and engagement channels and are owned and monitored by C&E. As such, C&E has the right to intervene to either moderate, reply or delete any social media activity within an official account. If this were to happen, C&E will let you know why this has been done.

Accounts exist for these reasons:

Neighbourhood policing accounts are used to:

- publicise local appeals to help detect and tackle crime
- create dialogue with the local communities they represent
- offer a visible presence for the public
- be accessible as a contact channel for the public
- inspire trust and confidence in the police

Operational policing accounts are used to:

- publicise local appeals to help detect and tackle crime
- offer a visible presence for the public
- inspire trust and confidence in the police
- demonstrate the breadth of operational work that specialist teams undertake

Chief Officer accounts are used to:

- inspire trust and confidence in the police
- reassure communities that the Constabulary is a cutting edge police force
- advocate and communicate the work that they are entrusted with from a national perspective

Miscellaneous accounts are used to:

- inspire trust and confidence in the police
- inform the public about specific information to help safeguard them from crime
- offer a voice piece for specific communities and hard to reach communities

Principles and expectations for affiliated accounts

Although affiliated accounts are owned by individuals, they are monitored by C&E. C&E is able to intervene to moderate, reply or delete any social media activity that may reflect the Constabulary in a negative way. If this happens, C&E will let you know why this has happened.



Social Media Policy

**Affiliated accounts are used to:**

- promote work that the Constabulary does to benefit the public
- show a more personal perspective of operational policing
- promote and highlight the messages from official accounts
- create dialogue with the local communities and partners
- inspire trust and confidence in the police



New - Request for a new Twitter account.



20170411-Corporate SocialMediaGuidance.

Previous policies can be found with the continuous improvement team.

Identification, Monitoring and Review

Security Marking:		NOT PROTECTIVELY MARKED / PROTECTED / RESTRICTED		
Document Title: Social Media Policy				
Type		URN	Strategic Board	Author/Reviewer
Policy			Monthly Executive Board	Rosh Patel
Version	Date	Changes (ensure public copy amended and uploaded to external website)		Complied with Policy Guidance ✓
	June 2017	DRAFT version – Version 1		
	July 2017	Draft version – Version 1.1 (consideration of comments made by Finance and actioned accordingly)		
	18 July 2017	Draft version – Version 1.2 (consideration of comments made by Finance and actioned accordingly)		
Next Document Review Date:				
EIA		EIA Sign Off		EIA Review
LOW				
SIA		SIA Sign Off		SIA Review



Social Media Policy



This version will be placed on the public domain website

If this version cannot be placed on the public domain website, provide reason and relevant COG authority