CLEVELAND POLICE

Social Media Policy

Policy Number	386
Policy Owner	Head of Directorate of Standards of Ethics
Version	1.0
Last Review Date	November 2022
Next Review Date	November 2025
Date of approval	4th October 2022
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	☒
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

Social Media Policy

1. Policy statement

Social Media is considered to be any website and application that enables users to create and share content or to participate in social networking. It is the fastest growing medium globally. People of almost every demographic group will use some form of a social media platform.

Social media has many benefits; making the world a smaller place, creating an environment for communities to come together and communicate. These benefits are shared by the Police service, enabling us to engage with the communities we serve far more effectively than we could prior to the phenomenon of social media. When conducted in accordance with the law and the Code of Ethics social media is a valuable tool in the prevention and detection of crime.

Despite the benefits, social media does have some consequences by creating forums that spread unethical or fake news. A contributory factor impacting on the wellbeing and mental health of people, particularly those that are young. Perhaps the greatest consequence is the ability to commit criminal activity through social media, such as the spread of terrorism, the supply of controlled drugs and other prohibited items and acts of harassment.

The use of such communications channels must be governed in order to ensure they are used most effectively, whilst maintaining and enhancing our reputation and professionalism.

Officers and staff must understand the standards of behaviour expected of them when using social media, both in a professional and personal capacity.

The policy seeks to align with the APP College of Policing guidance and is intended to assist police officers and staff to make good decisions and act responsibly, in a manner that will allow them to make safe and effective use of social media in both a professional and personal capacity.

2. Purpose

The purpose of this policy is to assist Cleveland Police users of social media and empower them to use it safely, effectively, and appropriately. To ensure that social media works for us, not against us. Whether Cleveland Police officers and staff use social media in a professional or personal capacity, it is used in a way that best represents our force, its values and commitment to public service.

Cleveland Police officers and staff must use social media having due regard to the Code of Ethics and the standards of professional behaviour by which

everyone who works in policing is expected to abide, in addition to any requirement demanded by law.

This policy highlights the expectations of all on and off duty conduct of officers and staff. This will include contractors, consultants, volunteers, and temporary staff. It covers all social media accounts used in a professional and personal capacity.

This policy will deal with the following areas:

- Corporate/Professional Social Media Use;
- Personal Social Media Use;
- Use of Social Media for the Purpose of Investigations and Vetting;
- Reporting Concerns for Breaches of this Guidance.

2.1 Reference

The term 'social media' covers a range of online communication tools and services. These allow individuals and organisations to communicate with each other online in a variety of ways.

This includes:

- Social networking sites (i.e. Facebook, Twitter)
- Video sharing sites (i.e. YouTube, increasingly Instagram)
- Photo sharing sites (i.e. Instagram)
- Audio sharing sites (i.e. Spotify)
- Online meeting platforms (i.e. HouseParty)
- Locations-based networks (i.e. FourSquare, Storify)
- Professional networking (i.e. LinkedIn)
- Instant messaging services (i.e. WhatsApp)
- Blogs (i.e. WordPress)
- Email/text messaging subscription services (i.e. RSS feed)
- Presentation sharing (i.e. Slideshare, Prezi)
- Forums
- Podcasts
- Dating sites

3. Underpinning procedures

3.1 Corporate/Professional Social Media Use

Social media can provide us with immediate contact and access to a large audience. It can help us update and inform the public and improve the visibility of our policing activity. It offers an opportunity to build trust and confidence in our work, making us more approachable and a trusted source of information and support. This helps us build a receptive audience for times when we need to

distribute, or seek, vital information. It also represents a great opportunity, when used effectively, for meaningful engagement with our communities.
There should be three main purposes for any social media activity in line with the NPCC National Local Policing Guidance:

- To achieve a tactical or operational objective;
- To change or influence the behaviour of our communities for the better;
- To build capacity and trust with communities.

To achieve this all Cleveland Police social media accounts should have a clear role and form part of a coherent approach and strategy. There should be clarity of purpose, function, and the desired outcomes for each account.

In order to achieve this Cleveland Police must be able to have control of any corporate accounts, be that of individual Police officer/staff accounts or business area accounts.

The creation of any new social media account will require the submission of an application to the Head of Corporate Communications. An application will need to provide evidence that the proposed account will:

- Create a benefit to Cleveland Police;
- Have clear objectives and expected outcomes;
- Demonstrate how it will achieve the objectives and expected outcomes;
- Demonstrate no other existing Cleveland Police social media account cannot already achieve the objectives or be able to achieve the expected outcomes;
- Have a nominated owner and manager of the account;
- Show who other than the nominated owner will have access to the account;
- Demonstrate how the account will be managed and monitored during periods of demand, leave or other such absence and out of hours.

There are four levels of professional accounts, in a tier structure.

Tier 1: One corporate Facebook, Twitter, Instagram and Linked In account, managed by Corporate Communications. Used for all force-wide, regional and national campaigns, and daily public engagement. Also missing individuals, and the vast majority of appeals for information.

Tier 2: Geographical accounts. Facebook and Twitter accounts which are pages linked to neighbourhood policing areas. Monitored and updated by business areas, and also updated by Corporate Communications.

Tier 3: Specialist engagement accounts. Monitored, updated by and responded to by a specialist business area i.e. Cleveland Police Dogs, The Engagement Team, @ClePolFootball, Cyber Crime.

Tier 4: Individual accounts, digital leadership. Professional digital engagement by force leaders and voices. Personally administered, managed and populated within a framework underpinned by the Force's Values and the Code of Ethics.

3.1.1 Application scrutiny

Application scrutiny and reviews will be conducted by Cleveland Police's Corporate Communications department.

The scrutiny and review processes will ensure:

- The application is reviewed by a dedicated decision maker, chosen by the Head of Corporate Communications.
- All successful applications accounts will be subject of a trial period, in which the account will be assessed against the stated objectives. The account 'owner' will be required to agree with the original decision maker how this evaluation will be undertaken and facilitated.
- Following a successful trial, an account will be subject of annual review.
- All owners/users must sign confirming they have read and understood this policy, strategy, guidance, and associated legislation.

3.1.2 Account ownership and access

All corporate social media accounts will be owned by Cleveland Police, not an individual. The accounts and passwords will be created by Corporate Communications. Owners or users of the account will not, in normal circumstances, be permitted to alter passwords. An exemption to this may be when the security of an account is believed to have been compromised. In such instances, a password may be amended by an account owner or user, but the details of the amendment should be communicated as soon as practicable to Corporate Communications.

These processes will allow Cleveland Police to have proper control and access to all corporate social media accounts.

3.1.3 Existing Corporate Social Media Accounts

It is known that a number of Cleveland Police accounts have been in existence prior to the implementation of this policy. It is expected that owners of these accounts will conduct a retrospective application with Corporate Communications. Transfer of ownership of the accounts should be made to Cleveland Police. If transfer of ownership is not possible or against the wishes of the account owner, the owner will be required to cease using the account as one that is connected to Cleveland Police.

3.1.4 Closing of Accounts

In accordance with this policy, any account that represents the Force **MUST ONLY** be, or have been, set up by Corporate Communications. *Accounts that are*

set up with Cleveland Police AND as a professional Tier 1, 2, 3 or 4 account without prior authorisation from Corporate Communications will be deleted.

Additionally, Corporate Communications reserve the right to review and close any accounts in line with national guidance or emerging trends in this field and/or where the use of that account is considered inappropriate or ineffective. In reaching such a decision, consultation must first have taken place with the account owner or their manager as appropriate in the circumstances.

If you have access to a corporate Facebook or Twitter account (Tier 1, Tier 2 or Tier 3 – further details of the tier structures can be found here) and you are leaving the force, then you must notify Corporate Communications so that we can revoke your access.

If you have an individual account (Tier 4) and wish to continue using the same account, you must contact Corporate Communications prior to leaving the organisation to allow for removal of the Cleveland Police branding and references, and so your username can be changed if it references the force.

You will need to provide a personal email address that will take over from your force email address for the account.

YOU MUST make it clear to your followers that you are leaving Cleveland Police, and that you are no longer tweeting/posting on behalf of the force.

Please note that you cannot change a corporate account to a personal account while still working for Cleveland Police. If you no longer want to run a corporate individual account (Tier 4), please contact Corporate Communications to remove the account.

3.1.5 Corporate/Professional Social Media Account Use

This policy does not seek to give guidance on the appearance of social media accounts or general usage. Corporate Communications guidance documents should be referred to in relation to these matters.

All Cleveland Police officers and staff should apply the same professional standards to their online communications as they would to their face-to-face, telephone or e-mail communications.

Every interaction we have using social media must be conducted within a legal framework to ensure that the public disclosure of information and/or images is lawful and proportionate.

Users of Cleveland Police accounts will only be permitted to access and use the accounts on Cleveland Police issued devices, such as mobile phones or work computers. Users will not be permitted to access accounts via personal devices. An exception may be considered if it is necessary to urgently address a matter linked to a form of threat, risk and harm. Any usage on personal devices should be reported to Corporate Communications.

Numerous Acts of Parliament provide a content in which information can be disclosed to the public including, but not limited to:

- Contempt of Court Act 1981
- Magistrates Court Act 1980
- Children and Young Person's Act 1933
- Coronial Act 2009
- Sexual Offences Act 2003
- Numerous Acts of Parliament and associated regulations, guidance (as amended or extended) and case law provide a context in which information may be disclosed to the public including, but not limited to:
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- Human Rights legislation (including the Regulation of Investigatory Powers Act 2000 as amended or extended) further prescribe what information can lawfully be conducted on public social media.

Laws around privacy, defamation and libel must also be considered with regards to information posted on public social media as well as copyright laws and not using images or footage that is not owned by Cleveland Police. For example, where an individual's social network content is associated (even if not formally linked) with a publication (e.g. a public comment) they may be liable for its content. Regulations and codes of ethics may also apply.

In addition, the Data Protection Act, the Freedom of Information Act and Human Rights legislation (including RIPA) further prescribe what information can lawfully be conducted on public social media.

Those responsible for using social media on behalf of the Force must ensure all interactions comply with the legal framework and the social media website/application's terms and conditions of use and codes of conduct.

This means that anyone with responsibility for Force social media accounts should closely monitor comments received on posts and hide/remove these if they are in breach of any law, including defamation, copyright, confidentiality, negligent misstatement, malicious falsehood, data protection and contempt of court.

If more information on media law is required, please contact Corporate Communications.

Whenever an individual uses social media for or on behalf of Cleveland Police that use must:

- Have a policing purpose;
- Reflect the force's core values;
- Be professional in style and tone, use appropriate language and be well written, with a high standard of spelling and grammar;

- Be consistent with the Cleveland Police tone of voice, which is straightforward, helpful, friendly, informative, in line with the force values, open and respectful;
- Have been carefully considered in terms of the impact of any posts, in particular in relation to victims and vulnerable members of our communities;
- Remain impartial and not endorse or promote products,
- Ensure any activity in relation political positions is not in breach of the standards of professional behaviour or law, such as purdah
- Not make posts that may discriminating or seek to deny individual right to practice religion. This does not prevent celebrating religious ideologies, this is acceptable.
- Not undermine operational, investigative, or criminal justice processes.
- Comply with data protection legislation;
- Respect confidentiality and copyright;
- Protect the privacy and integrity of colleagues and members of the public under the Human Rights Act 1998;
- Not be defamatory or libellous;
- Not Discredit the Police Service by undermining public confidence;
- This includes not liking, sharing, or posting material originally posted by other groups/people.

Journalists and the media will follow Cleveland Police social media accounts. Police officers and staff may find that they experience direct media enquiries to their account. Any such contact may be replied to, directing them to Corporate Communications. Corporate Communications should also be contacted by the account manager or users to make them aware of any enquiry that has been made.

Any intelligence that is reported by the public on a Force generated social media post, must have an Intelligence report created by the person who requested the content.

Any concerns that social media is being used by members of the public to target officers and staff for the purpose of harassment or criminal behaviour should be reported for purpose of safeguarding subjects of the behaviour. The force must consider if crime recording, and investigation should take place. Reports should be made via the normal crime reporting methods via the control room.

It is the responsibility of the individual requesting the post to monitor the comments for any intelligence. Corporate Communications are only able to monitor comments to either engage with the public or hide/remove comments that are deemed inappropriate.
Our pages clearly state crime cannot be reported through social media. If a crime is reported on a Force social media account, the individual should be directed to call 101 or to report online if appropriate, and in an emergency to always call 999.

3.1.6 Complaints made Against Police

On February 1st 2020 new legislation changed the definition of a complaint to:

Any expression of dissatisfaction with a police force which is expressed (whether in writing or otherwise) by or on behalf of a member of the public.

Cleveland Police has encouraged the public to not use social media as a platform to make a complaint against Police, as not all accounts are constantly monitored or screened for the purpose of receiving public complaints. Despite this, account owners or users may find that a complaint against Police is made via their account.

The information relating to the complaint should be directed to the Directorate of Standards and Ethics. Contact should be made with the person who has made the complaint signposting them to the correct process to make a complaint.

3.2 Personal Social Media Use

The Code of Ethics and Standards of Professional of Behaviour are clear in the demand for all Police officers and staff expected behaviour on and off duty.

As a police officer, member of police staff or other person working for the police service, you must keep in mind at all times that the public expect you to maintain the highest standards of behaviour. You must, therefore, always think about how a member of the public may regard your behaviour, whether on or off duty.

Police officers or staff members who discredit the Police service by undermining public confidence, whether on or off duty may be in breach of those demands and face disciplinary procedures and in the most serious of circumstances face criminal proceedings.

Members of the public are entitled to make a public complaint regarding a Police officer or staff member in relation to their off duty conduct, if the allegation was proven to be true or admitted, it would discredit the Police service.

Police officers and staff should be mindful that privacy and article 8 rights may not be a defence to an alleged breach in the standards of professional behaviour. This position is supported in case law, Lord Bannatyne's judgment of B, C & Ors v Chief Constable of Police Service of Scotland & Ors [2019] CSOH 48, the Outer House of Scotland's Court of Session. He stated the claimants (Police officers) were in a special position, since in entering the force they had willingly made themselves subject to the specific standards of conduct which govern police behaviour (as set out in the applicable 2014 Regulations) [165]. He characterised this as the officers having accepted a special limit on the scope of their right to privacy, which he defined as follows: "if [the officers'] behaviour in private can be said to be potentially in breach of the Standards in such a way as to raise doubts regarding the impartial performance of their duties then they have no reasonable expectation of privacy." Lord Bannatyne's conclusion suggest that Police officers agree to limit their privacy rights when they join the Police service.

Deleting social media posts that are considered to be breaches in the standards of professional behaviour will not be a defence.

With that in mind Police officers and staff members must be mindful of their conduct through personal social media use.

Police officers and staff members must:

- Use social media safely and responsibly;
- Not post or publish online or elsewhere, or offer for publication, any material that might undermine your own reputation or that of the policing profession or might run the risk of damaging public confidence in the police service. This may include distasteful humour at the expense of victims of crime and anti-social behaviour;
- Not confuse the true meaning of *banter* for acts of offensive, bullying and harassing posts on social media;
- Not support, follow or like social accounts that may undermine public confidence in the Police service; examples may include accounts that promote misogynistic and discriminative behaviours, anti-police accounts, accounts that seek to target individuals or groups through bullying and harassment.
- Not duplicate, copy, post or publish any Police information. Such an instance may be in breach of the standards of professional behaviour of confidentiality and a criminal offence under the Data Protection Act;
- Not post or publish information or content that could suggest any political affiliation between Cleveland Police and any Political entity;
- Not post or publish any images or videos of yourself, colleagues or the public whilst on duty, carrying out Police activities, in Police premises, Police vehicles or in uniform (whether on or off duty);
- Not post any details of any Policing activity that is going to take place, is taking place or has taken place; this would not include sharing an official Cleveland Police social media post.
- Ensure any social media use does not create a perception that the account is linked to Cleveland Police;
- Not create or use pseudo Police related accounts;
- Not undermine legal processes, outcomes and subjects of legal processes. This would include undermining judges, magistrates, Coroners, LQCs (Legally qualified chairs), defendants, witnesses and victims. Legal processes would include Criminal, Coroners, Civil cases and Police Misconduct proceedings.
- Consider individuals that they follow or are followed by. Where those individuals meet the criteria under notifiable association the following or being followed on social media meets the requirement to submit an association.

3.2.1 Business Interests

Police officers and staff members are entitled to carry out a business interest providing they have sought and obtained proper permission through the Business Interest Policy.

It is common for businesses to be promoted or conducted via social media platforms.

It is vitally important that Police officers or staff members do not use their position to promote their business interests.

Police officers and staff members must ensure any such business social media account does not use their position in the Police service to promote it, this may simply include information that the business owner or employee holds an alternative position within the Police service.

3.3 Abuse of Authority for a Sexual or Emotional Purpose

The Police service and public reasonably expect that Police officers and staff members do not abuse their position to develop relationships for a sexual or emotional purpose.

Any attempt to do so breaches the standards of professional behaviour and the most serious cases constitute a criminal act. Any act or attempt to do so triggers a mandatory referral to the IOPC.

Police officers and staff members must:

- Not use their position to develop a sexual or emotional relationship through social media such as dating websites, this may include using pictures or videos of themselves on duty or in uniform on their account;
- Not make contact with victims of crime or a person they have met in their role as a Police officer or staff member. This would include seeking to add a person as a friend on a social media platform, sending them messages or liking posts they have made;
- Declare any attempt by a victim of crime or person they have met in their role as a Police officer or staff member to develop a relationship with them. This would include such a person adding a Police officer or Police staff member as friend on a social media platform, or sending them messages. Simply rejecting or ignoring the contact will not suffice. IOPC guidance is clear any neglect in reporting the matter constitutes an abuse and requires a referral to them.

3.4 Use of Social Media for the Purpose of Vetting

Everyone within, working alongside or delivering service on behalf of the police service must maintain high ethical and professional standards, and must act with the utmost integrity. They must also be seen to maintain and promote such standards. A thorough and effective vetting regime is a key component in assessing an individual's integrity. It helps to reassure the public that appropriate checks are conducted on individuals in positions of trust. Vetting also identifies areas of vulnerability that could damage public confidence in a force or the wider police service.

Authorised Professional Practice (APP) Vetting provides information on the vetting procedures that will be applied by police forces in England and Wales. It has been developed to support the consistent application of the minimum national standards relating to vetting across the police service.

The vetting APP provides guidance to the Police Service on how to most appropriately administer this function, within its guidance is provided around vetting practitioner's use of social media as a tool to conduct vetting.

The APP states specifically around open-source checks for the purpose of vetting:

Forces should check content on publicly available social media sites for the purposes of service reputational reassurance, and to ensure that the applicant's online behaviour is compatible with the Code of Ethics or Standards of Professional Behaviour.

The applicant must use social media responsibly and safely.

The applicant must not have published anything that could reasonably be perceived by the public or by policing colleagues to be discriminatory, abusive, oppressive, harassing, bullying, victimising, offensive or otherwise incompatible with policing principles.

The applicant must not have published, or offered to publish, any material that might undermine their reputation or that of the policing profession, or might run the risk of damaging public confidence in the police service.

A proportionate approach should be taken in relation to such enquiries. Forces need not spend excessive time in researching. If the subject cannot be found in a reasonable time period, a 'no trace' conclusion can be drawn.

Those conducting open-source research should be trained to the appropriate standard in accordance with local procedures.

It is expected that vetting practitioners within Cleveland Police utilise social media as a tool to ensure robust vetting processes are in place. Guidance on how to do so should be taken from the Vetting APP that is most up to date at the time.

3.5 Social Media Use for the Purpose of Investigations

The Internet and social media can be used to support police investigations and can be a useful source of evidence and information. As criminals and Organised Crime Groups continually identify ways of exploiting the Internet to commit crime so law enforcement agencies can use the Internet as a way of tackling criminality. The Internet and social media can be used to support a wide variety of police activity including crime investigations, managing public order events, and missing from home enquiries. For this reason, their use as an investigative tool is encouraged, subject to compliance with the rules below and legislation/procedures relating to data access.

The NPIA have identified 5 levels of activity in relation to Internet investigation:

- Overt Open Source Investigation/Research
- Core Open Source Investigation/Research

- Covert Advanced Open Source Investigation/Research
- Covert Internet and Network Investigations
- Undercover Officer on-line/Covert Internet Investigator

Any member of staff can carry out investigations/research at level 1 using police registered computers. However, activity at levels 2 - 5 requires the ability to be able to evidentially capture material using non-attributable computers and therefore must only be carried out by those trained to the appropriate level using equipment appropriate to that particular level.

Staff who are considering conducting investigations/research using the Internet need to be mindful that such activity can leave a trace, or 'footprint', which can identify the device used and, in some instances, the individual carrying out the activity. They must therefore take precautions to protect both their own security and that of police systems. In addition, such activity, depending on the level, may require authorisation under the Regulation of Investigatory Powers Act.

The use of such powers is complex particularly to those inexperienced in this area of Policing. Where any doubt is in the mind of a Police officer or staff member on how to manage an investigation or navigates the regulations advice should be sought from the Covert Standards Unit.

Police officers and staff should not conduct any operational contact between each other on social media platforms, such as a third party messaging platform, that is not previously authorised by Cleveland Police and any such authorisation should ensure the communications are conducted on auditable work devices. This may include work issued mobile phone and laptops.

3.6 Reporting Concerns in Relation to Breaches of the Guidance

Where concerns are identified that a Police officer of staff member has breached the Standards of Professional Behaviour in relation to the use of social media, these should be referred directly to the Directorate of Standards of Ethics. Reporting should be preferable to done in writing via the departments email inbox.

In circumstances where it alleged a serious breach in the standards has occurred, such as concerns an abuse of authority has occurred for a sexual purpose or a death/serious injury has occurred following Police contact, linked to social media use, contact should be made without due delay via the Directorate of Standards on-call. The details of the on-call officer can be obtained via the Control Room Force Incident Manager.

4. Appendices

There are no appendices associated with this policy.

5. Compliance and monitoring

The Head of Directorate of Standards of Ethics is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Directorate of Standards of Ethics will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

6. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

The following identifies all version changes.

Version	Date	Reason for update	Author
1.0	Nov 2022	New policy published following approval	[redacted]