Social Media Policy

This document is part of North Yorkshire Police policy to which all Chief Constable personnel and the functions provided by the Police, Fire and Crime Commissioner are required to adhere.

This document sets out the policy and governance arrangements for North Yorkshire Police's use of social media by all our officers, staff and volunteers. It sets out a clear set of standards of professionalism and best practice to support the ambition that our use of social media will provide an effective two-way communication tool for engaging with our communities.

Policy Statement

The continued growth and popularity of social media presents an opportunity for the force to enhance the way we engage with the communities we serve in an online capacity.

The use of such communications channels requires a level of governance to ensure they are used effectively to reassure, warn and inform the public, whilst maintaining and enhancing our reputation and professionalism.

Officers, staff, and volunteers need to understand the standards of behaviour expected of them when using social media, both in a professional and personal capacity. Guidance and training associated with this policy are available.

This policy has been produced in line with APP College of Policing guidance and is intended to assist police officers, staff and volunteers 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.

This policy does not apply to ex-employees or to the social media accounts belonging to trade unions representing police staff, the Police Federation, the Superintendents' Association or any other national policing body.

Aims

The public expects police forces, police officers, staff and volunteers acting on the force's behalf, to act with integrity and impartiality whilst upholding fundamental human rights and treating all people with equal respect. It is important that the public's expectations are also reflected in our online presence. To support this, our social media policy aims to:

- Provide officers, staff, and volunteers with an understanding of the standards of behaviour expected of them when using social media, both in a professional and personal capacity.
- Establish arrangements for the monitoring and governance of the use of official social media accounts by officers, staff and volunteers.
- Clarify the legal framework within which officers, staff and volunteers must operate when using social media on behalf of the force.
- Provide clarity as to what is expected when using social media, both in a professional and personal capacity.

Principles

Our use of social media will at all times be:

- professional,
- honest,
- transparent,
- accountable,
- ethical,
- appropriate,
- proportionate
- justifiable in law.

We will also be bound by the terms and conditions of use and codes of conduct set out by individual social media sites and applications we choose to use both in a professional and personal capacity.

The general rule is that the same standards of behaviour and conduct apply online as would be expected in offline communications.

Compliance

This policy will be reviewed annually, by the Digital Communications team and approved by the Corporate Communications Lead.

Those using social media on behalf of the force have responsibility for ensuring they comply with the guidance outlined in this document.

Line Managers of those using social media on behalf of the force are expected to monitor usage and ensure their teams comply with the guidance. Effective line management in the use of social media across the force is critical in ensuring we maintain public trust and confidence.

Corporate Communications is responsible for informing line managers of the use of social media by their direct reports and for raising any associated performance management issues if necessary.'

The Corporate Communications team is responsible for training and advising users of the force's official social media accounts.

The Corporate Communications team is responsible to Local Policing for the governance and review of this policy.

North Yorkshire Police reserves the right to monitor or record all communication on social media, both on and off duty, by its police officers, staff, and volunteers.

Records of activity may be used by the organisation for the purposes of quality assurance, conduct, discipline, performance, capability and/or criminal proceedings.

Leaving the force

If an individual has access to an official social media account and is leaving the force, then it is the responsibility of the individual's line manager to notify Corporate Communications of the exit date for the individual via the digitalcommunicationsteam@northyorkshire.police.uk inbox as part of their exit process.

This will ensure that access to official accounts has been revoked.

This policy statement is open to public viewing from the NYP Website

Definition of Special Terms
N/A

Linkages

Other Documents:
Use of Instant Messaging for Group Chats Guidance
Corporate Communications – Social Media Subsite
MPS Use of Social Media (npcc.police.uk)
Media Relations (college.police.uk)
How to Block Searches of Your Facebook Profile (lifewire.com)

1. Supporting Guidance

1.1 Legal Framework

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.

Numerous Acts of Parliament provide a context in which information can be disclosed to the public including, but not limited to, Contempt of Court Act; Magistrates Courts Act; Children and Young Person's Act; Coronial Act; and the Sexual Offences Act.

Laws around privacy, defamation and libel need to be considered when posting on social media, as well as copyright laws and avoiding the use of images or footage not owned by North Yorkshire Police.

In addition, the Data Protection Act, the Freedom of Information Act and Human Rights legislation, including RIPA (The Regulation of Investigatory Powers Act 2000), further prescribe what information and activities can lawfully be conducted on social media.

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

1.2 Digital estate

North Yorkshire Police's 'official' social media accounts are managed through the force's social media management platform, Orlo. The current official social media accounts for North Yorkshire Police can be found on The Source.

For reference to 'personal' social media accounts please see Chapter Four.

Subject to approval from Corporate Communications, any accounts set up before January 2020 may continue to represent NYP and are not considered 'personal' accounts. Instead, these are classed as 'legacy' accounts and are covered by the requirements in Section 3.1.

Any accounts which are not classed as official or legacy must not in any way look like they are affiliated with North Yorkshire Police i.e., this could be through the name of the account; the cover photo/profile image; the account biography; the content posted by the account.

1.3 Intelligence or reports of crime on social media

On an official social media account:

- Any intelligence that is reported by the public on an official account generated social media post, must have an Intel report created by the person who posted the content or who requested the content.

- If content is posted by Corporate Communications at the request of an individual, it is the responsibility of the requester to monitor the comments for any intelligence. Corporate Communications are only able to monitor comments to either engage with the public or to hide comments that are deemed inappropriate or against our community guidelines.

2. Engagement and Legalities

2.1 North Yorkshire Police's use of social media for engagement

North Yorkshire Police's Corporate Communications strategy is managed and directed by Corporate Communications. This is designed to support the force's Control Strategy to keep people safe, protect the vulnerable, be there when the public need us, support operational needs and be visible to our communities.

Users must be aware of the potential effect on public trust and confidence in North Yorkshire Police when posting on social media and maintain a professional image ensuring our style and content is appropriate at all times.

The use of social media for engagement purposes by police officers, staff and volunteers, in a professional capacity on behalf of the force, is authorised by Corporate Communications following attendance and completion of the mandatory social media training.

All users of North Yorkshire social media accounts are required to complete the required training before they are permitted to access the social media account relevant to them and their area.

Once you have your line manager's permission to use an official NYP social media account, please contact the Digital Communications Team to arrange training.

Once the training has been completed, you will be provided with a licence and login details for our social media management platform, Orlo.

In accordance with this policy, the personal login details when access is confirmed must never be shared.

In accordance with this policy, the official social media accounts of North Yorkshire Police must only be, or have been, set up by Corporate Communications.

Accounts that are set up with North Yorkshire Police branding without authorisation from Corporate Communications will be deleted.

Any direct or clear breaches of this policy may result in a referral to Professional Standards.

2.2 Legalities

The law applies to social media platforms (e.g., Facebook and Twitter) as much as it does to any other form of publication.

The media may use what officers, staff and volunteers post on social media as an official quote from the force. Where an individual's social media content is associated (even though not necessarily formally linked) with a publication (e.g. a public comment in a news article) they may be liable for its content. Regulations and codes of ethics may also apply.

Anyone with responsibility for force social media accounts should also 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.

3. Social media for official use

3.1 Social media for official use

Police officers, staff and volunteers using social media in a professional capacity and representing the force are responsible for the content they publish. If the force becomes aware of any breaches of conduct on social media accounts, individuals may be subject to misconduct procedures.

Anyone using social media to post from an NYP official account, or a legacy account, must only ever do so through the social media management platform (Orlo) and not natively through the social media platforms themselves, unless in exceptional circumstances, e.g. technical problems with the social media management platform. In this instance this should be logged with the Digital Communications Team.

Any legacy accounts that continue to represent NYP must share their login details with the Digital Communications Team and update the team of any password changes.

3.2 Level 1 accounts

If you contribute to a forcewide social media account, for example, the North Yorkshire Police Facebook page or the @NYorksPolice Twitter account, the landing page is set up and managed by Corporate Communications and must not be edited.

It will include:

- Description of the area covered by the account, that being North Yorkshire and the City of York
- Emergency and non-emergency contact numbers
- Link to force website
- Profile picture will always be the force crest (unedited)
- Banner / cover photo will be representative of policing within North Yorkshire
- Link to Social Media Community Guidelines (Facebook)

3.3 Level 2 and Level 3 accounts

If you are part of running an area or department accounts, for example, @NYP_York Twitter or the North Yorkshire Police – Ryedale account, Facebook or Twitter accounts for jobs and careers, the landing page is set up and managed by Corporate Communications and must not be edited.

It will include:

- Description of the areas covered by the account
- Emergency and non-emergency contact numbers
- Link to force website
- Profile picture will always be the force crest (unedited)
- Banner / cover photo will be representative of the area covered
- Link to Social Media Community Guidelines (Facebook)

3.4 Content – public posts

Social media best practice guidelines are available to assist in formulating effective content for posting to social media. The following are prohibited from being posted:

- CCTV images/footage or photos of individuals without written approval from Corporate Communications (due to the tight governance that is required for this type of content)
- Wanted / missing appeals (due to the tight governance that is required for this type of content)
- Representing any personal opinions about policing matters
- Political or religious lobbying or canvassing
- Posts for the purpose of personal or commercial financial gain, for instance solicitation of business or personal services

- Offensive or obscene material, such as pornography or hate literature
- Using profanities, lewd or offensive language
- Any image not taken by the user unless permission has been given by those who maintain copyright. If permission is granted, it will still need to follow valid consent processes as per the requirements of the UK GDPR.
- Any details or information around a fatality, victim identity or suspects arrested or information that could lead to their identification
- Racist, sexist, defamatory, offensive, illegal or otherwise inappropriate material
- Illegal, fraudulent or malicious activities
- Annoying or harassing another individual

3.5 Content – private / direct messages

The direct messaging facility on any social media account that represents the force is disabled and must not be used.

If switched on by an individual and used, it is in direct breach of force policy and could result in disciplinary proceedings.

In the unlikely circumstances there should there be any interaction by a member of the public via the direct messaging facility on your individual account or on an area/department account, please advise as below:

"We are unable to respond to direct messages on this account. Please call 101 for further assistance. In an emergency, please call 999."

3.6 Social media moderation – public comments

We have a responsibility to ensure our official NYP social media accounts are free from defamatory language, abuse, hate speech (see 3.9 Media Law) and any content which could be in contempt of court.

As well as this governing what we post ourselves, these principles apply to comments on our accounts from the general public. Account users should monitor public comments and hide any comments which:

- Could identify a victim, witness or suspect by any means, e.g. name, address, school, place of work, relationship etc.
- Identifies a serving police officer or member of staff in a manner which potentially affects his/her personal safety threatens violence, is grossly derogatory, or is untrue
- Use offensive language (please note, profanity filters are in place on our force Facebook pages to limit offensive language)
- Could be perceived as threatening or abusive to any individual/s
- Could potentially put the force into contempt of court
- Constitute hate speech.

N.B. the functionality to hide comments is only available for Facebook, and where possible comments should only be hidden, not deleted. Instagram only has the functionality to delete comments, not hide them, so in this instance they can be deleted. This should always be done through the social media management platform so that we have an audit trail of the action.

Turning off comments

Facebook does offer the functionality to turn off/disable comments for an individual post, but this should only ever be done in the rarest of circumstances. For example, when opinions provided are grossly offensive or legally unsound (i.e. there is a substantial risk of significant prejudice of active proceedings).

The decision to disable comments must only be made in consultation with the Corporate Communications team. It must be recorded alongside the rationale and the reasons for doing so must be explained to the public in the post, so we are always acting in a transparent way.

3.7 Banning public users from official social media accounts

Sometimes an individual's behaviour on our force social media accounts may lead to a decision to ban them. In the first instance, the following guidance should be followed:

- Ask them to refrain from making inappropriate comments and share a link to our community guidelines.
- If they do not desist, provide a second warning and an explanation that if they continue to post inappropriately on our accounts they will be banned. You could also share a link to how to make a complaint (use your judgement if this seems appropriate).

If the individual continues to post inappropriately, contact the Digital Communications team and the team will review to make a decision around banning the individual. All decisions must be recorded.

No one outside of Corporate Communications should make the decision to ban an individual from our accounts.

3.8 Standards of behaviour - your professional profile

When using social media on behalf of North Yorkshire Police, officers, staff, and volunteers are expected to abide by the following standards of behaviour:

- Act with honesty, openness and transparency.
- Treat others with respect, courtesy and fairness: Be respectful to those who interact with you online and their opinions.
- Act with integrity: act according to the highest standards of professionalism, abide by police regulations and force policies, and challenge unacceptable behaviour if deemed necessary and report breaches to the Digital Communications team via the digitalcommunicationsteam@northyorkshire.police.uk inbox.

- Respect confidentiality: Only disclose information when legally allowed to do so and if necessary and proportionate.

- Social media software management tool: You must only access official NYP social media accounts through the Social Media Management platform. This can be accessed via a desktop or your force issued mobile phone. Once you have your line manager's permission to use an official NYP social media account, please contact the Digital Communications Team to arrange training. Once the training has been completed, you will be provided with a licence and login for our social media management platform, Orlo.

- Password sharing must not take place. Usernames and passwords for official social media accounts and log ins for Orlo are not to be disclosed to any other person. If a password compromise is suspected, it must be reported immediately to the Digital Communications team and the Information Security team via the established incident reporting processes, as per our Incident reporting procedure.

- Mobile phones/electronic devices: In line with force policy, only force issued mobile phones or electronic equipment may be used to access force social media accounts, do not use personal devices*. You must only use a personal mobile phone or electronic device to access personal social media accounts, do not use force issued electronic equipment*.

*Exemptions apply. On rare occasions, members of the Corporate Communications team may need to use personal devices to access official social media accounts to protect the reputation of the force (for example if they notice a mistake, out of office hours, that has the potential to be reputationally or operationally damaging but that can be quickly rectified from their personal account rather than calling out the on-call representative). The Corporate Communications Lead should always be notified by email in this instance.

3.9 Procedure during a major or critical incident

- In the event of a major or critical incident, such as a terrorist attack or mass public disorder, it is important that the force's forcewide social media accounts and other online channels become a trusted source of accurate information and that everything issued is clear, appropriate and can be legitimately classed as our official comment (see JESIP principles and the Critical Incident Procedure).

- In this instance all accounts should cease posting (with the exception of the forcewide NYP Facebook and Twitter accounts which are controlled by Corporate Communications.

- If necessary, Corporate Communications will use the Social Media Management Platform to deactivate all accounts except the forcewide channels. In this case, users will be advised by a message on the dashboard of the social media management platform. Corporate Communications will reactivate accounts with the authority of the commanding officer when safe to do so.

- This is to ensure that the public, stakeholders and the media can quickly and easily identify important communications from the force and that local/specialist accounts do not unwittingly post something inappropriate, inaccurate or irrelevant.

- This procedure reduces the many different avenues for the public reporting into the force using social media, meaning that Corporate Communications – can focus on monitoring and replying to the public exclusively on those accounts.

- In recognition of the valuable role that local accounts can play in reassuring communities in the aftermath of such an incident, deactivation of these accounts will be implemented for the minimal time necessary and users trusted to engage with their local communities in line with the Gold communication strategy.

3.10 Media law

All the force's social media content is covered by British media law and the same rules apply to North Yorkshire Police as they do to the news media and the general public.

The main legislation users must be aware of is:

- Defamation

  Defamation occurs when someone makes a false statement about an individual or group of individuals which causes reputational damage if published or broadcast.

  There are six defences against Defamation based on strict criteria and conditions

  In the context of police use of social media, risks include publishing posts which infer or suggest guilt at a point when nothing has been proven in law, publishing comments not heard in open court, publishing information about someone that cannot be proven as true, naming someone at the point of arrest, and sharing defamatory comments from another social media account onto one owned by North Yorkshire Police

- Contempt of Court Act

  Contempt occurs when something is published or broadcast publicly which creates a substantial risk of serious prejudice to active legal proceedings.

  In the context of police use of social media, this means that from the point of arrest onwards, nothing should be published or broadcast which could influence a jury and affect a suspect's right to a fair trial.

  Risks include: posting detailed information about the circumstances of a crime after someone has been arrested or charged, posting information which infers or implies guilt or blame, posting information about a suspect's previous offences, posting personal opinions about anyone subject to ongoing criminal or legal proceedings.

- Children and Young People Act

A breach occurs if a child under the age of 18 years is identified while concerned in legal proceedings either as a victim, defendant or witness, unless a court order has been imposed to lift this protection.

Information regarded as identifying a child includes name, address, school, a still or moving image, any other information which could be used alongside the above to identify that child.

In the context of police use of social media, risks of a breach include naming an under-18 charged with an offence or appearing at Magistrates, Youth or Crown Court, naming an under-18 who is or has been in court where a Section 49 order or Section 39 order has NOT been lifted.

- Copyright

Copyright protects an individual's creative work and is automatic. It covers creative writing, art, illustrations, photography, video, audio, web content, film and TV recordings and broadcasts, and graphic design.

Breaches occur when any such work is copied, distributed (including on social media), replicated or adapted without the owner's written permission.

Risks for police use of social media include: taking images or videos from Google or other search engines where the creator has not granted copyright-free use, using images from a manufacturer or retailer's website of stolen goods or of vehicles used in a crime as an illustration.

3.11 Retention of personal data within social media posts

'Personal data' is any information about a living individual which allows them to be identified.

Identification can be directly using the data itself or combining it with other information which helps to identify a living individual.

In the context of what we post on social media it can include, but is not limited to:

- A custody photograph and/or name and/or address of an individual shared at the end of criminal proceedings
- A photograph and the personal details of a missing person or a wanted person
- CCTV images of an unknown individual

The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and other legislation relating to personal data and rights, such as the Human Rights Act.

Posts containing personal data will be taken down after the period of time outlined in the Corporate Communications' retention policy.

It is the responsibility of the person who drafted or requested the posting of the content to ensure that the content is removed.

3.12 The use of social media for intelligence and investigations

Please refer to the Internet Intelligence and Investigations (Triple i) Procedure- which you can also find on The Source.

It is not the responsibility of Corporate Communications to contact witnesses and victims through social media.

3.13 Closed / private Facebook groups

We must be open and transparent about our use of social media.

You should not use a Facebook group in your capacity as a North Yorkshire Police employee unless:

- You are a digital PCSO and are conducting community engagement in that group as agreed by the group admin.
- You are a member of the Digital Media Investigation team.

If you wish to access a social media group or individual profile for investigative purposes, please contact the Digital Media Investigation team.

If you wish to access a social media group for the purposes of community engagement or any other purpose, please contact Corporate Communications who will be able to advise on this.

4. Social media for personal use

4.1 Content and posting to social media accounts

In line with Police Staff Conduct Guidance, you must not include the following employment-related information on your personal public profile or any additional pages you have set up in a personal capacity:

- Posting of information or images you have accessed in the course of your duties (unless this has been shared on an official account)
- Images (still or moving) of non-public areas of police premises
- Use geo-location to post your location on social media in any police buildings
- Posting or sharing of any material or links to any material that is defamatory against the force, another organisation or individual that could bring the force into disrepute
- Posting or sharing of any material or links to any material that could be deemed to be offensive, inappropriate or illegal.
- Publication of force crest, email address, landline, mobile, official force artwork or anything else that would suggest to the public, media, and other stakeholders that your account is linked to NYP or representing NYP in any capacity.

4.2 Use of instant messaging apps for group chats

The use of instant messaging apps such as WhatsApp and Facebook Messenger are commonplace in society. There are set restrictions in place for the use of such apps on North Yorkshire Police devices, however it is known that personal devices will also be used to message and share between members of North Yorkshire Police.

Guidance is in place to assist members of North Yorkshire Police understand the expected standards when using instant messaging. The procedure is not restricted to any one service / app and is to be applied to all types.

You can access the guidance here: Use of Instant Messaging for Group Chats

4.3 Your safety

In line with APP College of Policing guidance, it is **recommended** that police officers and police staff do not include the following on personal social media profiles:

- Employer details
- Details of job role
- Images of uniform
- Mobile telephone numbers
- Home addresses
- Personal email addresses
- Family members' details
- Hobbies and places frequented
- Details of vehicles
- Sensitive information such as racial and political views
- Images of colleagues without their consent
- Vetting level obtained and maintained as part of your role

This is guidance only and is provided for safety reasons. If you make the decision to include any of the above information you should be aware of the following subsequent risks:

- Risk to public trust and confidence in North Yorkshire Police (associations with any inappropriate content)
- Risk to prejudicial investigations if operational materials/tactics are revealed
- Increase vulnerability to harassment, corruption or blackmail
- Risk of being a potential terrorist target
- Breach of Data Protection Act 2018

In line with College of Policing guidance, police officers, police staff and police volunteers using personal accounts are responsible for the content posted on their profiles/accounts. If the force becomes aware of any breaches of conduct on social media accounts, individuals may be subject to misconduct procedures. If you have any concerns about a colleague's use of social media, please email Professional Standards or report using the anonymous messenger.
Please consider the risks associated with identifying yourself as a member of the police service on your profile - we would encourage officers, staff and volunteers to speak to PSD about personal security related to social media and your data.

4.4 Standards of behaviour - your personal profile

When using social media for personal use, officers and staff are expected to consider the following standards of behaviour:

- Disclosure of information: police officers and police staff members are reminded that their employment contract stipulates that information gained in the course of their duties should not be disclosed outside the force otherwise than in accordance with their duties.
- Privacy settings: police officers and police staff members are issued with guidance on recommended privacy and security settings for social and digital media accounts for personal use. They are advised to follow these recommendations in order that their privacy and account security is protected.
- Treat others with respect, courtesy and fairness: be respectful to those who interact with you online and their opinions.
- Mobile phones/electronic devices: you must only use a personal mobile phone or electronic device to access personal social media accounts, do not use force issued electronic equipment to access personal social media accounts*.

*The exception to this is the Corporate Communications team, some of whom have their personal social media accounts, linked to the forcewide Facebook accounts.