If printed, copied or otherwise transferred from the policy library this document must be considered to be an uncontrolled copy. Policy amendments may occur at any time and you should consult the Policy library if in doubt.

Social Media Policy

Reference Number	5/20	**Version**	8
Department Responsible	Corporate Communications		
Author	Kelly Noble		
Senior Owner	Richard Edmondson		
Effective Date	12 March 2020	**GSC Marking**	Official
Type	Policy	**Review Date**	27 April 2024
Date Last Reviewed	27 April 2023	**Reviewed By**	Kelly Noble

1. Introduction

Northamptonshire Police uses social media to effectively engage with the residents of Northamptonshire, with the aim of increasing trust and confidence in the police. Social media enables us to support operational policing, generate intelligence in response to appeals, share information, and is an additional tool in the detection and prevention of crime. This policy applies to all police officers, police staff, special constables, volunteers and cadets who use social media in a professional capacity to represent the Force.

2. Legislative Compliance

This document has been drafted to comply with the principals of the Human Rights Act. Proportionality has been identified as the key to Human Rights compliance, this means striking a fair balance between the rights of the individuals and those of the rest of the community. There must be a reasonable relationship between the aim to be achieved and the means used. Equality and Diversity issues have been considered to ensure compliance with current Equality Legislation and policies. All Equality, Diversity and Wellbeing considerations have been recorded in the accompanying Equality Impact Assessment (EWIA) which is stored within the Force Policy Library system. GDPR, Data Protection and Freedom of Information issues have been considered. Adherence to this policy will therefore ensure compliance with all legislation and internal policies.

3. Policy Statement

Contents

1. Statement

Northamptonshire Police uses social media to effectively engage with the residents of Northamptonshire, with the aim of increasing trust and confidence in the police. Social media enables us to support operational policing, generate intelligence in response to appeals, share information, and is an additional tool in the detection and prevention of crime.

1.1 Content and Scope

This policy applies to all police officers, police staff, special constables, volunteers and cadets who use social media in a professional capacity to represent the Force.

1.2 Ethics

Anyone employed by or volunteering for Northamptonshire Police using social media for work purposes should ensure posts comply with the College of Policing's Code of Ethics.

This states that you:

Ensure nothing you publish online can reasonably be perceived by the public or your policing colleagues to be discriminatory, abusive, oppressive, harassing, bullying, victimising, offensive or otherwise incompatible with policing principles

And

That you do not 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.

1.3 Aims of Social Media Usage

Northamptonshire Police aims to utilise its social media accounts to:

- Prevent and detect crime
- Develop a wider contact and engagement channel
- Provide real time interaction with the communities of Northamptonshire
- Engage with targeted audiences, hard to reach communities and key influencers
- Manage the flow of public information during major incidents through concise and timely message delivery
- Dispel rumours, provide the facts and be a trusted voice
- Improve the public's trust and confidence in the police
- Break down barriers and traditional stereotypes associated with police forces
- Enhance the reputation and integrity of the Force
- Extend the Force's visibility and accessibility online
- Enable the Force to reach and engage with a wider audience
- Ask questions and gain feedback from the public
- Monitor public tone and sentiment about specific issues, incidents and events

- Promote campaigns, appeals, initiatives and share good news stories
- Use paid social advertising to target specific audiences

There are five primary 'Northamptonshire Police' branded accounts, as well as four neighbourhood team Facebook pages, all listed below. There is also a large number of Twitter accounts ran by officers and staff.

Facebook: Northamptonshire Police
Twitter: @northantspolice
Instagram: @northamptonshirepolice
LinkedIn: Northamptonshire Police
YouTube: Northamptonshire Police

Facebook: Kettering and Corby neighbourhood team
Facebook: Daventry and South Northants neighbourhood team
Facebook: Wellingborough and East Northants neighbourhood team
Facebook: Northampton neighbourhood team

2. Social Media Accounts

2.1 Requesting a Social Media Account

The following procedure must be followed by anyone requesting a new social media account or access to an existing account:

1. Email Corporate Communications at news@northants.police.uk outlining what type of social media account is required or which account you would like access to, including your rank/position and an outline of how you intend to use it
2. Corporate Communications will review the request and either send a return email or speak to you directly
3. If you haven't used the social media channel before, you will be expected to attend some training before being approved, and you will be required to read the relevant social media guidance
4. Once approved, the account will be set up by Corporate Communications. If an account is refused, a reason will be provided as to why
5. It is your responsibility to add your profile photo and bio, which both must represent your role within the Force
6. Corporate Communications will set a password for your account and let you know what it is - if you change this for any reason, you must inform the team immediately so they can update your password which is kept in a secure folder
7. Passwords must not be disclosed to anyone other than Corporate Communications

2.2 Account Names

Social media usernames are to be named based on the role, the team or the area that the account represents. All accounts must be easily identified as being part of the Northamptonshire Police network, this includes using relevant names, descriptions in the bio, correct branding, collar numbers and use of the Force crest.

2.3 Account Usage

If a social media account is approved, there is an expectation that the account holder/or team will update the account regularly and monitor comments and messages.

There is not an enforced minimum or maximum number of posts a day, but your account should not simply be used to monitor and retweet other accounts. Further guidance on this is below in section 3.3.

Social media usage should not detract from day-to-day work. Equally, it will only be effective if used frequently. Accounts will be closed if they have not been used for 60 days, unless appropriate mitigation can be provided.

Accounts will be monitored for usage and to ensure only appropriate content is being published. If an account is used inappropriately, posts will be removed, the individual will be contacted and guidance from Corporate Communications will be offered. See section 3 for further guidance.

2.4 Twitter Accounts

Northamptonshire Police has many individual officer Twitter accounts as well as team/department accounts.

If you have an individual officer account, you should remember that the primary purpose of these Twitter accounts is to highlight your role within the organisation and this should always remain the core content.

Group Twitter accounts should only be used to post information relating to the work of the department/team and share other Force account related content. They should remain professional, informative and engaging at all times.

Guidance for users on the general use of Twitter is available in the Twitter Q&A document available on ForceNet under Departments > Corporate Communications > Social Media Guidance.

Corporate Communications keeps a record of all Force Twitter logins and passwords. If you change your password, you must let the team know what it is immediately so they can update the records.

2.5 Facebook Admins

The Corporate Communications team are the main admins of the Northamptonshire Police Facebook page. Officers in the Force Control Room and Missing Persons team also have access to post on the main Northamptonshire Police Facebook page via Hootsuite, mainly so they can publish information outside of the working hours of Corporate Communications where the threshold of contacting the on-call press officer is not met.

The Neighbourhood team Facebook pages are managed by PCs, PCSOs and Sector Coordinators. Corporate Communications are also admins on the page to oversee activity and provide guidance where necessary.

Following the relevant training (provided by Corporate Communications) and if it is relevant for their role, officers can be added to a neighbourhood Facebook page via the admin function. Individuals are given admin access via their personal Facebook profile which must be an active account. Login is via this Facebook profile however, this link between the personal account and professional page cannot be seen publicly. Only other admins will see other admins who manage the page.

Access can be revoked should an individual breach the social media policy. Guidance for admins on the general use of Facebook is available in the Facebook Q&A document available on ForceNet under Departments > Corporate Communications > Social Media Guidance.

2.6 Instagram, LinkedIn and TikTok

There is only one Northamptonshire Police Instagram account and LinkedIn page and both are used by Corporate Communications only. Anyone who would like content added to these platforms should contact Corporate Communications who will decide if it is relevant.

If you'd like to take part in a team/department Instagram takeover for a day, contact Corporate Communications who will provide guidance and any training beforehand.

Northamptonshire Police does not have a TikTok account representing the Force. It is against policy to set up an TikTok account on behalf of Northamptonshire Police and if you use the platform for personal reasons, you should avoid identifying yourself as a police officer.

2.7 Use of WhatsApp

Northamptonshire Police Policy Surrounding the use of WhatsApp

The use of WhatsApp and other instant messaging applications has been reviewed by both the Independent Office for Police Conduct and National Policing Information Risk Management Team in 2020. These reports highlighted concerns about the use of WhatsApp. The report identifies risks, impacts and lessons to be learned so that appropriate policies and guidance can be applied where the use of such services are sanctioned/supported by Force or organisations.

In light of these reports, Northamptonshire's Police's position has been reviewed and we continue to not sanction or support the use of WhatsApp. The app is not available to download from Play store onto Force issued devices. Any use of WhatsApp that is happening on personal devices, is not permitted to be used for policing data. This is in line with the Information Security Policy.

It is acknowledged that WhatsApp is in widespread use for social networking, and people socialise with work colleagues.

It is not for Northamptonshire Police to dictate whether you use it on your own phone for this purpose but everyone should be aware that the content should not in any way be policing data – about people, incidents, processes, buildings, staffing, sickness or anything else relating to the business of policing.

You should be mindful about any private conversation on non-corporate channels 'drifting' into a discussion about official matters. For example, a discussion about a social event drifting into a discussion about a work meeting. At the point that the discussion becomes about official business, you should use official communication channels. Or at the very minimum, you should forward the official part of conversation to an official system.

Any data breaches carried via WhatsApp could result in disciplinary or legal proceedings.

Anyone choosing to use it is expected to take personal responsibility for complying with policy and procedure, including Information Security Policy and other Information Assurance related policies (e.g. Data Protection/GDPR, Records Management, Freedom of Information) as well as this Social Media Policy.

In 2022, the Information Commissioners Office (ICO) conducted a review into government use of private correspondence channels, including WhatsApp, following messages that were leaked by ministers and officials during the pandemic. The investigation found that the lack of clear controls and the rapid increase in the use of messaging apps and technologies, including WhatsApp, had the potential to lead to important being lost or insecurely handled. The ICO concluded that there were real risks to transparency and accountability. Their guidance states that any official business should be conducted through corporate communication channels such as departmental email accounts, wherever possible and that official information exchanged through private channels should be transferred on to official systems as soon as possible.

Public officials should be able to show their workings through proper recording of decisions and through the Freedom of Information Act, to ensure that trust in those decisions is secured and lessons are learnt for the future.

The advice below is offered to help you make informed decisions about your personal data and group membership:

- No-one should be required to join a group as part of their job – it is your device and your personal data and as such it remains your choice as well as your responsibility
- Know who the members are, and who the Group Admin(s) is/are, and importantly be aware that profile data including your personal phone number are visible to others in the group
- If you are a Group Admin, remove people or close a group when it is no longer needed. If it is for an event, close it when the date has passed; if it is a group of work colleagues consider what happens when someone leaves a role or the organisation
- Familiarise yourself with the app settings and adjust them accordingly, including who can see your profile and where group images are stored.
- The app is owned by Facebook and data may be shared between apps (usually for targeted advertising) including sharing with other countries. **REMEMBER:** UK Data Protection laws may not apply to any data you share with/via WhatsApp
- WhatsApp security disclaimer states that the service is not warranted as secure or safe

When using the app consider the following issues:

- Previous security issues with WhatsApp have resulted in messages and media being accessed and potentially shared by third parties.
- Anyone with access to your phone can see your messages, including a preview of messages on your lock screen. Be mindful of who has access to your device and where you leave the screen visible and unattended.
- There are other instant messaging (IM) products that are supported for business purposes, such as MS Teams Chat and Cisco Jabber.

WhatsApp security updates are issued regularly; you must update the app and ensure these updates are consistently applied

*Any requests for installing WhatsApp on a business mobile device will be declined by D&T. Anyone wishing to explore having the app approved needs to seek support of an Information Asset Owner (usually a Supt or Head of Dept).

2.8 Guidance on the Personal Use of Social Media and Online Dating

Social media

The huge growth in the public use of social media sites over the last few years has provided significant new opportunities to make contact with the communities we serve. These platforms including Facebook, Twitter, Instagram and TikTok are also used extensively by police officers and members of police staff in their private lives.

We know that the vast majority of our staff act with integrity and apply professional standards of behaviour throughout their service but sadly there will be some who don't and this puts them at risk of disciplinary action and damaging the reputation of the Force.

The Standards of Professional Behaviour state that police officers and police staff should behave in a manner which does not discredit or undermine public confidence in the police service, and that includes how you behave online, and on your personal social media accounts.

- The same standards of behaviour and conduct apply online as would be expected offline

- Remember that information placed on the internet or social media could potentially end up in the worldwide public domain and be seen or used by someone it was not intended for, even if it was intended to be 'private' or in a closed group

- Officers and staff should avoid using social media off duty after consuming alcohol or when judgement is impaired

- Pause before you post - we can all get frustrated and we would ask that you pause before posting your frustrations on social media. Sending something in the heat of the moment can result in complaints and grievances and there are processes in place internally that can deal with your frustrations professionally and in the right way

- Ensure your social media profiles are set to private and keep on top of your personal security settings

- Due caution should be paid when updating such sites with personal photographs, comments and 'check-in' information. Regardless of how rigorous your security settings are, if someone from your circle of friends chooses to share the information, you instantly lose control of it and are unable to determine who else sees it. This could put your safety, that of your family and operational integrity at risk.

- Make sure you are familiar with other related Force policies including Information Security, Data Protection Act and use of email/internet

- Remember that what you like and share reflects on you - liking or associating yourself with social media sites and content that is inappropriate could compromise you and your ability to carry out your duties as a police officer or member of police staff. It can also lead to a complaint against you. You could be putting your career at risk by associating with inappropriate people, groups or organisations both in person and online

- Report any concerns you have about a victim or witness making unwarranted contact with you via social media. You should not engage in conversation and report this to your supervisor.

Online Dating

While online communication has many benefits and can help us to engage effectively with our communities, these channels can also expose officers and staff to inappropriate contact with criminals, victims, witnesses and members of the public, and that includes online dating sites.

We want to be clear that we are not stopping officers and staff from using online dating sites but we are keen to prevent the sending, sharing or posting of inappropriate images and/or photographs on those dating websites. This includes inappropriate images of staff, officers and PCSOs in uniform (or parts of their uniform). We want officers and staff to use social media and online dating sites safely.

2.8 1) Social Media Influencers

Increasing numbers of people are being approached as 'social media influencers' to promote products or services for gain. Anyone who works for the Force who profits from their personal social media account or posts, or has a paid partnership with a business, should register their activity as a business interest with PSD beforehand. Be mindful of any approaches and the nature of them, do not identify yourself as a police officer and always adhere to our social media policy guidelines.

3. Appropriate Content

It's important to keep our social media accounts regularly updated to ensure they are an effective tool in ongoing communication with the public.

It's equally important that the information and updates that are posted to the channels are appropriate and accurate. Images or information posted on any social media site by any officer, staff or volunteer must be legitimate, necessary and proportionate. Adherence to the Social Media Policy and the Social Media RAG document will help to ensure compliance.

3.1 Appropriate Use of Social Media

Corporate Communications is responsible for monitoring and creating content for the five primary, 'Northamptonshire Police' branded accounts listed in Section 1.3.

The team in Corporate Communications will also check the usage of other social media accounts within the Northamptonshire Police network on an ad hoc basis. However, the team is not responsible for replying to any comments, issues or complaints as the responsibility lies with the account owner or admin.

Corporate Communications will check these accounts for:

- Output on the account, accounts should be updated regularly with fresh and engaging content
- Posts that could be seen as inappropriate
- Any training issues

Remember that all posts and updates on social media must have a policing purpose. Please read the Social Media RAG available on ForceNet under Departments > Corporate Communications > Social Media Guidance. This provides a traffic light guide as to what content you should and should not be posting on social media.

3.2 Posting Photos

When posting photos as part of your social media posts, please take into account the following:

- As with words, photos must remain professional and not compromise ongoing activities or investigations or bring the organisation or yourself into disrepute
- Always get consent for photos you take that feature people. Photos featuring individuals or small groups must not be posted on social media without their consent. For large groups of people, consent is not required – e.g. fans attending football games or a photo of a busy town centre or street. Any photos that are going to be used for any marketing campaigns or for public use, always gain consent and let them know exactly where they will be used
- Photos of anyone under 18 should not be used without parent or guardian consent - if in doubt of any photo, ask for consent to share and tell them exactly where it will be shared
- If your photos include colleagues, you must check they are happy for you to share on social media before you publish - also be mindful about who is in the background of your photos
- Do not identify offenders or victims in photographs

- Do not publish photos of knives and bladed items – this can glamourise usage and worry the public unnecessarily
- Think not only about what is in the foreground of your photo, but whether there is any restricted information shown in the background
- You should not post, or digitally manipulate images, you are not the copyright holder of or do not have permission to use

Use common sense, think before you post and always seek permission. Contact Corporate Communications for further guidance on photo use. Please read the Social Media RAG for further guidance.

3.3 Inappropriate Use of Social Media

As well as monitoring accounts on an ad hoc basis, the Corporate Communications team will also check accounts where an issue has been raised to them, either by a member of the public, an officer or a staff member. The team will check for any content that may be seen to be inappropriate or could put the Force into disrepute.

If it's deemed that an account is being used inappropriately, the relevant post(s) will be removed, the individual will be contacted and advice will be given. The issue may also be raised with the individual's line manager.

Please read the Social Media RAG document which outlines all of the topics that you are not permitted to post to any social media account.

Your account should not be used to:

- Share details about your personal life
- To sit dormant and monitor other accounts
- To solely retweet other Force accounts
- As a competition to see who can get the most followers

If it is used for any of the above, you will be contacted by Corporate Communications with guidance and your account may be deactivated.

3.4 Posting Appeals on Social Media

Witness appeals must be dealt with by Corporate Communications and posted to the relevant social media pages. Individual account holders or anyone with access to social media pages are advised not to post appeals to social media, unless they are very low level and:

- Impact on the community has been considered
- The appeal does not identify premises, victims, or witnesses
- It does not include images or descriptions of suspects arrested
- It does not breach contempt of court legislation

Important: If account holders wish to use social media appeals, they must be shared or retweeted from the main accounts.

Do not copy the appeals and/or create a new post about an appeal or missing person. By only sharing appeals from the main social media accounts, this will ensure that when the original posts are removed, all shares will be automatically deleted.

This is because, once a suspect has been identified, an arrest has been made and/or charges have been laid, or a missing/wanted person has been located, all content and images relating to that individual must be removed from the public domain as soon as possible.

All appeals (content and images) should be removed after 30 days. On the first day of each month (or nearest working day), the Corporate Communications team will go through Facebook and Twitter to ensure all appeals are removed.

3.5 Posting Arrests and Charges on Social Media

Social media users must consider the impact on the community and the Force when posting arrests on social media as well as ensuring that the content is legally compliant, the post does not name the suspect(s), does not imply the suspect(s) are guilty and does not hold the individual or the organisation in contempt of court. If unsure, seek advice from the Corporate Communications team.

Users are not permitted to post details of arrests or charges on social media. If there is a large amount of interest from the community or a specific need for a charge to be published on social media, account holders should contact Corporate Communications and seek permission to post the charge on social media.

3.6 Dealing with Major Incidents

In the event of a major or critical incident, it is important that the Force's social media accounts become a trusted source of accurate information and that everything issued is clear, appropriate and can be legitimately classed as our official comment.

In this instance all accounts should cease posting (with the exception of the main Northamptonshire Police accounts which are controlled by Corporate Communications) until further notice.

If necessary, Corporate Communications will stop any planned and scheduled social media posts from going out to ensure that the public, stakeholders and the media can quickly and easily identify important communications from the Force.

With a large national incident or operation, for example, Op London Bridge, there may be a communications plan that will be circulated and resources will be made available to social media users. This will include any messages and images you should publish on your Force account or page.

3.7 Reporting Suicide on Social Media

Do not use your account to discuss suicide in any way. This is a sensitive subject and discussing the subject matter publicly can have a significant impact on people with mental health issues.

The Corporate Communications team will release appropriate information on this topic when required and will abide by these safe standards for the coverage of suicide. 10 top tips for reporting suicide | Samaritans' media guidelines

3.8 Images and Copyright Law

All social media users need to be aware of copyright law. If an individual wishes to post images, videos or sound recordings of any kind on social media they must ensure they seek the permission of the person(s) who owns the copyright to those products and that any license restrictions or stipulations are adhered to.

Account holders are encouraged to use photographs they have taken themselves or the communications products developed and provided by Corporate Communications.

3.9 Pre-election Period of 'Purdah'

As an organisation, Northamptonshire Police must remain politically impartial at all times. In the pre-election period known as Purdah, all officers and staff members must be very careful not to do or say anything that could be seen, in any way, to support any political party or candidate.

This includes sharing or posting political content and having photos taken with any party members. This applies to local, general or European elections.

4. Monitoring

The account holder is responsible for monitoring their social media account. Monitoring of the account includes reviewing and replying to comments and private messages, as well as removing or hiding comments where necessary.

4.1 Monitoring of the Main Force Social Media Accounts

Corporate Communications is responsible for monitoring the five primary Northamptonshire Police social media accounts listed in section 1, for any interaction that is public facing e.g. comments, mentions, replies, as well as interacting with other accounts. The social media accounts will be monitored Monday to Friday between the hours of 8am and 5pm.

4.2 Monitoring of All Other Force Social Media Accounts

All other social media accounts must be monitored by the account holders and those who have access. Individuals should monitor the replies and comments as well as any private messages.

4.2 a) Replying to Comments and Tweets

It is highly likely that members of the public will comment on and reply to posts. Social media is a platform that provides a method of two-way communication and users are encouraged to respond and communicate with members of the public through designated social media channels.

Account holders should endeavour to reply to any query or issue raised, they should also act on complaints received or direct to the appropriate channel.

If a social media post generates a high number of comments and replies, or if the individual is unsure how to respond to comments, they should contact members of the Corporate Communications team who will provide advice and guidance.

4.2 b) Turning off Replies and Comments

If you need to restrict comments altogether on a post, you can turn them off or limit the audience for them. On Facebook, this can be done once the post is published by going to the three dots on the post and choosing 'who can comment on post' and change to 'profiles and pages you mention'. On Twitter, go to 'who can reply' and change to 'only you'. On Instagram, the same process applies again, and then go to 'turn off commenting'.

4.2 c) Replying to Direct Messages

Twitter and Instagram both allow members of the public to send private or direct messages. These messages need to be monitored and replied to.

If a member of the public is trying to report a crime via social media, they should be directed towards the relevant reporting methods.

If the message is related to an issue in the local area or seeking general safety and crime prevention advice, the account holder should endeavour to answer these or pass on a relevant email address.

4.2 d) Freedom of Information Requests

All Freedom of Information requests received via social media will be valid where it provides an applicant's name and address for correspondence and a clear request for information.

The decision as to whether it is a valid FOI will be made by an FOI Officer. All FOI requests should be directed to freedomofinformation@northants.pnn.police.uk.

Requests for explanations, clarification of policy, comments on the public authority's business etc. are not valid FOI requests.

They can also be guided to the website here: **www.northants.police.uk/foi-ai/af/accessing-information**

4.3 When to Remove Comments

An account holder has grounds to remove or hide comments posted to a social media platform if:

- It could identify a victim, witness or suspect by any means, e.g. name, address, school, place of work, relationship etc.
- It 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
- Offensive language has been used
- It could be perceived as threatening or abusive to members of the community
- It could potentially put the Force into contempt of court.

If an account holder has to remove a significant number of comments, they should post a comment explaining why the content has been removed and provide a link to the public social media guidelines on our website to remind members of the public that certain behaviour or language will not be tolerated by Northamptonshire Police.

Below are some instances when removing comments must be considered and actioned where necessary. Please contact Corporate Communications for further clarification if unsure.

In addition to this, the team will take action and remove any posts or comments, posted by officers, staff or volunteers, which breach social media guidelines.

Twitter will only allow a person to remove their own content. Comments cannot be deleted by other users.

4.3 a) Defamation and Libel

A statement about a person is defamatory if it tends to do any of the following:

- Expose the person to hatred, ridicule, or contempt
- Cause the person to be shunned or avoided
- Lower the person in the estimation of right-thinking members of society generally
- Disparage the person in his/her business, trade, office or profession.

4.3 b) Contempt of Court

Although every individual has the right to Freedom of Speech, it's important to ensure that comments on a social media post would not affect court proceedings and/or create bias that could affect a judge or jury's opinion or decision such as discussions of previous convictions or anything that implies guilt.

Furthermore, if incidents or arrests are posted on social media, the account holder must remove comments which mention names or identify the arrested person.

If the account holder removes a comment, they should add their own comment with a polite warning that posting the names of individuals is in breach of Northamptonshire Police's public social media guidelines and those comments will be removed.

4.3 c) Hate Speech

Hate speech is any language which targets a protected characteristic in a derogatory manner.

In terms of social media, this could be a comment made which is perceived by the victim, or any other person, to be motivated by hostility of prejudice based on a person's actual, or perceived, disability, race, religion/faith, sexual orientation and/or transgender.

Any comment that is seen to be hate speech should be removed by the account holder. If the hate speech continues then a comment should be added by the account holder, explaining why comments have been deleted along with a reminder of Northamptonshire Police's public social media guidelines.

If the individual continues to post inappropriate content the account holder may consider blocking that user, see section 4.4 Blocking Accounts, for more information.

4.3 d) Offensive and Threatening Language

All Force Facebook pages have the profanity filters activated which blocks offensive language, however, there may be instances where offensive and threatening language needs to be removed manually by the account holder.

Comments should be removed if they include profanities (curse or swear words) or language which constitutes hate speech (see section 4.3 c Hate Speech).

Comments should also be removed when the content is deemed to generate substantial risk of harm to an individual, if it's grossly offensive or if threatening language is used which incites violence or threatens the life of another individual.

It is important to note that Twitter does not have a profanity filter and tweets cannot be removed, however, accounts can be blocked where necessary and appropriate. Please see section 4.4 Blocking Accounts, for more clarification.

4.3 e) Spam/Repeat Comments

If a Facebook user is posting spam comments such as website links or promotional content for a profitable organisation, these comments should be deleted. If the spam content continues, the account holder may consider blocking that user, see section 4.4 Blocking Accounts for more information.

If an individual is repeatedly posting the same comment on a Facebook page, whether this be written content, an online article, video, etc. the account holder may want to try and engage with the user, attempting to resolve the issue or answer their query. If the duplicate comments continue, remove the duplicates, leaving only the original comment remaining.

Tweets to your Twitter account from other users cannot be removed, however, where appropriate, accounts can be blocked, see section 4.4 Blocking Accounts for more information.

4.3 f) Operationally Sensitive Information

If any Facebook user mentions operationally sensitive information which could compromise an investigation or affect a covert operation, the comment should be removed immediately.

As mentioned, Twitter doesn't allow you to remove tweets from other account so you would not be able to remove this information on Twitter.

4.4 Blocking Accounts

There may be grounds to block an individual for the reasons mentioned in Section 4.3. If an account holder feels an individual should be blocked, they should contact the Corporate Communications team for advice before taking action.

If you feel that it is appropriate, you can try and engage with the user and give them a warning before blocking.

It is important to keep a record of blocked users, so you should take screenshots that include the name of the individual, the comments made and record the reasons why they have been blocked. One you have taken screenshots, you can then hide/delete the comments on the platform and block the user.

4.5 Reporting Offensive Content as a Crime

Offensive or threatening content on social media should be reported when it falls into these four categories of criminal offence:

- Credible threats to a person's life, safety, or property
- Communications targeting specific individuals, including persistent harassment and ongoing abuse
- Breach of court orders, e.g. identifying people protected by law
- Communications which are grossly offensive, indecent, obscene or false.

If any police officer or staff member finds content that they consider to be of this nature on social media, they can report it as a crime, following the normal procedures.

4.6 Trolls

Internet trolls are social media users who deliberately try to disrupt, attack, offend or generally cause trouble with the online community by posting certain comments, images or other online content.

There may be grounds to block an individual from the social media platform for the reasons mentioned in Section 4.3.

If the content they are posting is offensive, threatening or abusive, you may need to consider removing comments (if on Facebook) and blocking the account, refer to section 4.3 and 4.4 for more information.

5. Social Media Security

If you are using a social media account to represent the Force, it is important that you take social media security seriously and regularly look at the security and privacy settings of your account.

- Remove all third-party applications linked to social media profiles and accounts unless absolutely necessary
- 2 Factor Authentication can seriously reduce the risk of any breach occurring in the first place and is recommended by social media companies as best practice
- Follow National Cyber Security Centre guidance in the use of passwords and how to avoid phishing attacks
- Use of personal email addresses and personal phones for business use is likely to increase security vulnerabilities
- Change passwords regularly, ensuring they are complex and unique. When you change passwords, force log out of all devices
- Activate alerts for new login attempts from other devices and browsers

Actions to take in the event of a social media hack of your corporate profile:

- Inform Corporate Communications
- Report security breach immediately in accordance with local force security procedures. Ask that the National Management Centre is informed.
- Engage with your local Information Management team. When it is suspected that personal data has been compromised a decision will need to be made whether to report to the Information Commissioner's Office.
- Report your account as compromised to the relevant social media channel.
- Notify the NPCC Social Media lead (office hours only), as they can assist and liaise with Facebook/Twitter directly.
- Change all passwords immediately, on all channels, not just the one that has been hacked.
- Start an incident log and timeline of events.

- If a single profile was hacked then remove them as admin.
- Contact all personal accounts linked to any compromised page and ask them to force log out of all sessions and ensure they have 2FA switched on.

6. Governance

The Corporate Communications team use a social media management system called Hootsuite. Th system allows the team to manage and schedule social media content, as well as monitor activity on all channels.

Hootsuite enables the Corporate Communications team to have oversight of all of Northamptonshire Police's social media accounts and manage in one place. The platform also allows the Force Control Room and Missing Person Team to sign in and have access to post on our main Facebook and Twitter accounts when the Corporate Communications team are unable to.

7. Policy Adherence

All employees and volunteers for Northamptonshire Police are required to abide by this this policy. Non-adherence may result in referral to line managers and/or PSD as appropriate.

The publishing of content which is deemed to be inappropriate may lead to the referral to a line manager and or PSD where appropriate. Accounts may be frozen and/or removed by Corporate Communications.

Users of accounts which have been frozen for 'non-adherence' will be required to undergo further training by a member of Corporate Communications before their account is returned.

8. Leaving the Force

If you are leaving or transferring to another Force, you must notify Corporate Communications so they can update the records of users that have access to that specific account or close down the account completely.

You must also make it clear to your followers that you are leaving Northamptonshire Police and that you are no longer tweeting on behalf of the Force.

Please note that you cannot change a corporate account to a personal account while still working for the Force. If you no longer want to run a corporate individual account, please contact Corporate Communications.

4. Monitoring and Review

The senior owner will review the content of this guidance annually to ensure that this is relevant and up to date. The author has agreed that this document will be reviewed within 12 months of the effective date.

5. Related Documents

All available on Forcenet under Departments > Corporate Communications > Social Media Guidance.

Facebook Q&A

Twitter Q&A

Social Media RAG

Public Social Media Guidelines

6. Document Control History

DATE	VERSION	INDIVIDUAL	CHANGES MADE
13 March 2020	1	Kelly Noble	
16 March 2020	2	Kelly Noble	EWIA changes
14 April 2020	3	Kelly Noble	EWIA changes
15 April 2020	4	Kelly Noble	Update to policy
17 June 2020	5	Kelly Noble	Update to policy
1 November 2021	6	Kelly Noble	Update to policy
11 March 2022	7	Kelly Noble	Update to policy
27 April 2023	8	Kelly Noble	Update to Policy