POLICY

Digital and Social Media

Policy Owner	Corporate Communications
Policy Holder	Digital Media Lead
Author	Vanisha Mistry
Policy No.	41

Approved by

Legal Services	Under review
Policy Owner	16 June 2017
JJNCC	7 June 2017

Note: *By signing the above you are authorising the policy for publication and are accepting responsibility for the policy on behalf of the Chief Constables.*

Publication date	16 June 2017
Review date	16 June 2020
APP Checked	9 November 2015
College of Policing Code of Ethics	9 November 2015

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation specific to the subject of this policy document

Act (title and year)
Computer Misuse Act 1998
Contempt of Court Act 1981 (Reporting restrictions)
Magistrates Court Act 1980 (S.8 Reporting restrictions)
Youth Justice and Criminal Evidence Act 1999 (Reporting restrictions)
Sexual Offences Amendment Act 1992 (Reporting restrictions)

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
H&S Legislation
Data Protection Act 1998
Freedom Of Information Act 2000

Other Related Documents

- ACPO Guidelines on the Safe use of the Internet and Social Media
- College of Policing 2017 draft APP on Relationships with the Media
- ICT Strategy

1. Introduction

1.1 The aim of this policy is to ensure appropriate use of digital and social media for engagement purposes. The policy is designed to act as a guidance framework and outline corporate communication standards around the use of social media accounts by our officers and staff, at work and out of working hours.

1.2 It also defines the procedures for applying for access to a corporate social media account, its management thereafter and the security and safety procedures relating to both the recording/loading of information and loss of associated equipment.

1.3 Both Forces will strategically use social media to establish a clear vision for policing. The importance of all social media must be recognised and every effort will be made to increase its use in a proactive manner to meet wider business objectives.

1.4 This policy has been developed for both forces to ensure a consistent and appropriate use of digital and social media. As such it replaces the Digital and Social Media policy v1.

2. Background

2.1 The use of digital and social media is increasingly important in all areas of policing. It supports the ever evolving policing landscape and has opened up a multitude of platforms which Norfolk and Suffolk Constabularies can use to enhance communication with the public.

2.2 As the appetite for online services, information and interaction continues to increase, Norfolk and Suffolk Constabularies recognise that traditional methods of communication may have less impact and limitations in potential reach. Embracing digital and social media opportunities is no longer desirable but essential.

2.3 Easy access to technology and the growing use of mobile internet means that an online presence is part of everyday life. Norfolk and Suffolk Constabularies' ICT Strategy advocates a 'digital by default' approach, ensuring the Constabularies evolve and develop in line with the changing communications preferences of the public.

3. Definitions

3.1 What is digital media?

Digital media refers to audio, video, and image content which has been encoded (digitally compressed). It includes computer programs and software, digital imagery, digital video, video games, web pages and websites, social media, digital audio and e-books.

What digital media platforms do both Constabularies use?

- Websites
- Video
- Images
- Social media

3.2 What is Social Media?

For the purposes of this policy, social media is defined as:

"Computer-mediated technologies that allow the creation and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks."

3.3 What social media channels do both Constabularies use?

Both Norfolk and Suffolk currently have access to, and use, the following platforms:

- Twitter
- Facebook
- Vimeo
- Google+
- Instagram

Other applications available within these platforms are also available for use, e.g. Facebook Live/Periscope.

Any staff wishing to use these additional facilities must seek prior agreement from Corporate Communications and sign off from their Departmental Head.

3.4 New digital and social media channels will become available over time. To ensure central oversight of any new engagement, all trials on new channels must be requested and approval sought via the Digital Media

Lead (DML) in line with this policy. Any requests that may not be covered through the policy will be presented to the DML, who will then take this to the Deputy Chief Constables for decision.

3.5 Focused social media events around police operational activity should be carried out with the approval of line management and in prior consultation with Corporate Communications. This will ensure messaging is consistent with the existing strategy and all digital and social media channels have been considered for the wider promotion of the event.

4. Aims and Objectives

4.1 Norfolk and Suffolk Constabularies' corporate digital and social media accounts aim to provide:

- A source of important information about Norfolk and Suffolk Police
- An opportunity for members of the public to engage with the constabularies
- A potential reduction in demand on other areas of the organisations, where appropriate
- Increased trust and confidence and stronger relationships with local communities
- An opportunity for dialogue via online methods
- Engagement with members of the public on platforms that are socially acceptable in the wider digital aspect
- Effective publication of operational information, e.g. news and appeals
- Responsive, accurate and timely updates on key events and incidents

5. Benefits

5.1 The benefits of Norfolk and Suffolk Constabularies' digital and social media presence are as follows:

- Promotion of Norfolk or Suffolk Constabularies in an alternative way to that of traditional media, delivering user preference;
- Enhanced management of major incidents through improved message delivery and managing third party comment/rumour;
- Engagement with and response to the communities of Norfolk and Suffolk Constabularies online about policing and community issues, in order to cut crime and help build confidence in the service;

- Enabling and supporting users to embrace new technology and tools to empower communication and engagement;
- Channelling users to the Constabularies' websites, thus potentially reducing demand in other areas of business;
- Developing an online community and building relationships with local audiences.

6. Management of Content

6.1 The following sections offer general guidance to digital and social media users. Corporate Communications can provide additional and more detailed support and should be contacted with any queries.

6.2 Accuracy: all digital and social networking, blogs and video sharing sites must be accurate, up-to-date and relevant, with a regular flow of new content to maintain user interest.

6.3 Account management: the Corporate Communications department will have access to all sites and will be capable of removing inappropriate material. All login account details must be forwarded to the Digital Media Team who will maintain a list of all accounts. Changes to login details and passwords must be passed to the Digital Media Team at the time the changes are made. Any applications added to social media accounts by Corporate Communications must not be deleted.

6.4 Complaints: any serious complaints, issues, discrepancies or breach of this policy or accompanying guidance with any force accounts will be referred to line management in the first instance and Information Security and/or the Professional Standards Department, as appropriate.

6.5 Direct Messages: Officers using individual corporate social media can expect a degree of privacy regarding direct and private messages. For the purpose of auditing or a complaint, Corporate Communications have authority to access an individual's direct messages. Dependent on the nature of the audit or complaint, direct messages may also be accessed by line management, Information Security or the Professional Standards Department for auditing, performance management or disciplinary purposes in line with the E-mail, Intranet and Internet Policy.

Users are reminded that direct and private messages may still be made public (by the recipient or through account compromise) and should therefore operate on this principle, ensuring content remains professional and appropriate at all times.

6.6 Live major incidents: messages about incidents managed by CID, Public Protection Unit, Major Investigation Team or other live major incidents must not be communicated on any social media channel, except with the express authority of the Senior Investigating Officer (SIO), with approval documented for auditing. Full responsibility for social media messages

about these incidents remains with the SIO, CCR and Corporate Communications department. Corporate Communications and / or the Contact and Control Room (CCR) may instruct social media users not to use their accounts while a major incident is in place: strict adherence with such requests is essential.

During a major incident, officers may re-tweet/share messages from the main corporate accounts or provide localised reassurance messages on agreement from Corporate Communications. If in doubt, please contact CCR or respective news teams (x2722 Suffolk; x3666 Norfolk) for guidance.

6.7 Corporate and personal social media accounts should not be used to send messages about operational matters to other officers: the accounts are there to communicate with the public. In particular, Twitter should not be used to communicate with other officers about tasking or resourcing issues.

6.8 Before posting on any social media channel, operational staff should consider whether it is necessary to issue any information about live or sensitive incidents (the A-Z pocket handbook should be referred to). On some occasions there will be a need to post information, for example, to alert the public to road closures due to a road traffic collision; however, detailed information should not be posted. This may be because resources are still being mobilised, facts of the incident are yet to be clarified or next of kin need to be informed.

6.9 It is the responsibility of the district, department or individual posting photographs or footage to ensure that they comply with legal or data protection requirements and, if necessary, a risk assessment and/or Equality Impact Assessment (EIA) should be carried out. Photographs and footage that could compromise an operation or investigation or jeopardise a court case must not be posted.

6.10 Media queries or questions raised as a result of an officer or member of staff tweeting are the responsibility of that officer or staff member to respond to. Requests for interviews should be directed to the news team in order to maintain a corporate position on issues: the news team will identify the most appropriate person to make a response.

6.11 Uploading any information to digital and social networking sites is a form of disclosure and therefore must comply with data protection principles. Officers and staff should also ensure that they are familiar with the Freedom of Information Act 2000.

6.12 Users should be aware that traditional media such as newspapers, local radio and regional TV use social media to gather information about policing. This may include personal details, telephone numbers, e-mail addresses and links, images and interests. Officers and staff should be aware of this in relation to their personal social media accounts as well as in their use of corporate accounts.

6.13 The media are entitled to report on anything tweeted from a corporate account: any such content is covered by Qualified Privilege which means that the media are not liable for any inaccuracies or actionable content.

6.14 All officers and staff must note that any comments made on digital and social media will be deemed to be in the public domain and treated as official police comment. Any comments could therefore be liable to a misconduct severity assessment. This applies to both personal and corporate sites.

7. Surveillance Images

7.1 Digital and social media is an efficient way for forces to engage with the public and ask for assistance with key policing issues such as missing persons and unidentified offenders. If used correctly, it can be of great benefit and successfully develop public confidence in policing.

7.2 Police forces now have access to a wide range of surveillance images through technologies such as CCTV. However, there have been some incidents where images have been posted to social media by the police where questions of public confidence and organisational reputation have been raised and scrutiny of the 'policing purpose' has ensued.

7.3 Images that have been obtained by forces must have a legitimate policing purpose and, if they are to be posted on digital and social media, it is important that it is proportionate and justified, especially if it is an image of a person. This relates to any living individual that is identifiable. When handling such images, officers and staff should be reminded that they must adhere to Data Protection principles, such as retaining only for a necessary period and being shared appropriately.

7.4 The Information Commissioner's Office (ICO) has a CCTV code of practice, which can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

8. Wanted/Missing People

8.1 Any appeals for wanted or missing people should not contain images in the messages but instead link to the main website www.norfolk.police.uk or www.suffolk.police.uk so that images can be removed promptly and effectively once people are detained or found. District, departmental or individual accounts should not post their own appeals for wanted or missing people: contact Corporate Communications for assistance.

8.2 Photographs of wanted people, including custody photos and CCTV appeals, should not be posted directly onto social networking sites.

9. Setting-up, closing & monitoring corporate accounts

9.1 Applications for new corporate accounts are managed by the Corporate Communications department.

9.2 Before any digital or social media account (used as an engagement tool or non-covert) is established, officers or staff must have approval from their line manager and Head of Department.

9.3 Any officer or staff member across Norfolk or Suffolk who wishes to open an account must send an email request to Corporate Communications: corporatecommunications@norfolk.pnn.police.uk (the team covering both forces is managed from Norfolk) with a short outline of their aims and objectives, the purpose of the account and what digital or social media channel they are proposing to use.

9.4 All staff requesting the use of any digital and social media channel should familiarise themselves with this policy and any other appropriate guidance documents.

9.5 All requests will be reviewed and approved on an individual basis by the Digital Media Lead. The Digital Media Lead may consult with the member of staff and suggest alternative platforms, based on their requirements.

It should be noted that Chief Officers have agreed that both Constabularies will no longer create individual social media accounts apart from those that were set up prior to January 2017. New accounts will be considered within the following remit:

- Department
- Specialist area
- Team
- District

9.6 When an account has been approved, Corporate Communications will set up the account on behalf of the department or area, ensuring that it fits with the corporate brand and style.

9.7 Under no circumstances should any member of staff attempt to set up or use their own digital or social media account.

9.8 All social media accounts must have their usernames and passwords registered with the Digital Media Team to ensure that accounts can be protected and recovered if hacked.

9.9 Officers and staff must inform the Digital Media Team when they change their password, name of account or owner of the account at the time of its change.

9.10 The Digital Media Team may change passwords at any given time, should they believe there is a security risk. The Digital Media Team will ensure they inform all the relevant people of the change.

9.11 Accounts must not be closed by users without prior consultation with Corporate Communications. It is important to inform the public, and in turn any followers, that the account is being closed and that there is an alternative communication platform that they can access.

9.12 Any police officer or staff member who no longer wants to have an official account must inform the Digital Media Team and their line manager. The Digital Media Team will then implement the closure of the account, if appropriate, or liaise with their line manager/department head to find alternative staff to continue the account.

9.13 All digital and social media accounts must be used regularly in order to be effective. Corporate Communications will monitor usage and, if accounts are not used for three months, will offer users guidance and, if required, training to encourage activity. If accounts are unused for six months, a reminder will be sent. After a further month, Corporate Communications may close an account if the user does not make contact.

9.14 Line managers are responsible for monitoring and supervising the content of the account. If their team is responsible for a social media account (district accounts, for example) they are ultimately responsible for its content.

9.15 Corporate Communications will regularly monitor public messaging on all corporate social media accounts to ensure compliance with policy and guidelines, and will offer guidance to officers, where appropriate. Line managers will be responsible for monitoring the accuracy and relevance of local content. Relevant senior leadership teams are responsible for the overall governance of local content in consultation with the Corporate Communications department.

9.16 All organisation accounts and their content (including individual accounts set up prior to Jan 2017) remain the 'property' of – and under the governance of – the Constabulary. Accounts cannot be converted into individual or personal accounts without the prior consent of the Digital Media Lead or Deputy Chief Constables.

10. Account Security

10.1 Corporate use: Norfolk and Suffolk Constabularies' corporate social networking and video sharing sites will be administered by the Corporate Communications department.

Any lost Constabulary-owned phones, computers or other devices with access to Norfolk or Suffolk Constabularies' digital or social media accounts should be reported to both ICT and Information Security immediately. Corporate Communications should then be informed so that the account can be protected.

A Staff member using a mobile device to access digital and social media should ensure all additional security layers are implemented. For example, always use the screen lock function.

Passwords should not be changed by anyone other than a member of the Digital Media Team unless in exceptional circumstances; for example, an account is compromised and the password needs to be changed with immediate effect. Corporate Communications must be informed of any changes immediately.

10.2 Administrator & Digital Media Team use: The Digital Media Team based in Corporate Communications will have access to all force digital and social media accounts (including individual Twitter accounts) and have the authority to remove inappropriate posts/material or suspend accounts.

The administrator of any social media account is responsible for the management of the account's password. The administrator should observe appropriate security levels in relation to these shared account passwords. Administrators should keep details of all staff members with access, and change passwords when team membership changes. Once a password has changed, administrators should email the updated password to the Digital Media Team at webteam@norfolk.pnn.police.uk or webteam@suffolk.pnn.police.uk

Staff should be careful about adding applications to social media accounts as they will often be granting access to account information to a third party provider, and may therefore compromise the security of their account.

If third party apps are used, staff should ensure they read the small print before signing up. For example, any photos added to Twitpic are then owned and can be used by Twitpic.

To protect the reputation of the Constabularies, as well as protecting the reputation of its employees, officers and staff should not set up or contribute to unofficial or spoof police groups, pages or accounts.

11. Social Media Training

11.1 Officers and staff who apply to use a corporate Twitter account must attend a Twitter/Social media masterclass before they begin to use the account. Should a course not be immediately available they should ensure they attend the next available class. Any existing users should attend the next available Masterclass. In addition, all social media users must attend an annual refresher session to share best practice, ensure consistency of use and be made aware of any revisions to guidelines. Failure to attend a masterclass or refresher session may lead to social media accounts being suspended.

11.2 Ad hoc training and guidance is available from Corporate Communications. Members of the team are trained to provide advice and support all officers and staff in relation to corporate social media sites. The digital media team can provide one-to-one sessions on using different

social media accounts: email webteam@norfolk.pnn.police.uk or webteam@suffolk.pnn.police.uk. The news team can provide advice on legal issues surrounding content and potentially sensitive information: email pressoffice@norfolk.pnn.police.uk and media@suffolk.pnn.police.uk

12. Use of Personal Devices

12.1 Norfolk and Suffolk Constabularies do not have a 'Bring Your Own Device' policy. An exception has been made by Chief Officers on the basis that officers and staff are able to use their own personal devices to update corporate social media accounts. A record of those using their own device to update social media accounts should be kept by the individual's line manager.

12.2 Whilst it is acknowledged by the Constabularies that officers and staff may choose to use their own personal devices to update their corporate social media accounts, users are reminded to be careful about the security of their own equipment.

Officers and staff are also reminded that they must not connect their own personal devices to force network computers: further guidance around this can be found in the Information Security Policy.

13. Private Use of Social Media

13.1 All officers and staff are accountable for any information placed in the public domain, even if it is a privately held account.

13.2 Due to potential risks to the security of the user's personal information and that of their family and their friends, all officers and staff should be aware of the need to protect themselves and their personal information online whilst using personal social media accounts.

13.3 As such, officers and staff are urged to ensure that security settings on social media accounts are set to the maximum for personal safety.

13.4 When posting information on social media sites, both personal and corporate, consider the risks:

- The personal safety and exploitation of personal information – avoid providing addresses, phone numbers, email addresses etc.
- The security of the organisation.
- The security of information relating to family, friends and other contacts.
- The welfare, safety and privacy of colleagues, customers/next of kin.
- The integrity of operations and investigations.
- Any indirect reference to the user's role or the organisation on personal accounts.

- When using a mobile device, consider turning off any GPS/location tracking options within social media apps that identify the user's location.

13.5 During election periods, officers and staff should not post comments to express a political opinion on their personal sites – this is particularly important during the election of Police and Crime Commissioners.

13.6 Any comments made on personal sites should not reveal confidential police information, including personal data or information which might jeopardise any operational policing matters.

13.7 Officers and staff are advised not to make reference to Norfolk Constabulary or Suffolk Constabulary on personal social media accounts. Any activity on personal social media accounts which seeks to ridicule or is overtly critical of the Constabularies, officers or other staff is strictly prohibited.

13.8 When using private social networking, blogs and video sharing websites, Norfolk or Suffolk Constabularies' name, crest or insignia must not be used without the express permission of the Corporate Communications department. Consideration must also be given to any other matters of copyright.

13.9 All officers and staff are accountable for information they publish, even on privately held accounts. Inappropriate use or inappropriate disclosure of personal information on digital, social networking and video sharing sites is subject to criminal proceedings in accordance with s55 of the Data Protection Act. It is a criminal offence to disclose personal information unlawfully and/or misconduct procedures.

13.10 Officers and staff who upload personal details to social networking, blogs and video sharing websites should be aware that they are placing personal details into the public domain. This may impact on their own privacy, the security of family and friends and, in particular, may compromise their vetting status or ability to be deployed on certain types of policing such as undercover or covert operations.

13.11 When using private social media sites, staff are advised not to make any comment or post any images of behaviour which are, or could reasonably be perceived to be, beliefs or conduct that are contrary to the expectations of behaviour outlined in the Standards of Professional Behaviour.

13.12 The same standards of behaviour and conduct apply online as would be expected offline – even if the information is intended to be 'private'. Officers and staff are advised against using the internet and social media off duty after consuming alcohol or when their judgment may be impaired.

13.13 Individuals should make no reference to their employment within either Norfolk or Suffolk Constabulary on their postings nor should they post any

work based photographs or information concerning their employment. Once an individual is identified as working for the police their vulnerability increases and the potential for compromising their 'friends' who are also work colleagues increases.

13.14 Officers and staff are advised not to make adverse comment regarding their police force, colleagues or senior managers or the police service in general on the internet or social media and are advised to make use of internal facilities to vent any such comments.

13.15 It is advised to always restrict your settings/privacy settings/profile information/contact information appropriately and to check your account settings if new features are enabled. For example, on Facebook, you can allow ‘only friends’ to view your profile and messages rather than ‘everyone’.

13.16 Be careful about disclosing private information that may compromise your safety or that of your family, friends, associates or employer.

13.17 Officers and staff deployed on covert or other operations are strongly advised to disable LBS and GPS services on personal ‘smart’ phones and to avoid the unintentional disclosure of their location through the posting of images on the internet or social media.

13.18 Be mindful that you may be targeted as an employee of Norfolk or Suffolk Constabulary by criminals who wish to gain your trust and then take advantage of that trust for criminal purposes.

13.19 You should not display photographs of yourself in your Constabulary uniform, post any inappropriate images of staff in uniform, on police premises or performing unacceptable activities.

13.20 Your Constabulary email address must not be posted on your profile or used to register any personal social media accounts.

13.21 You should always consider how joining a “group” may reflect on you and the Constabularies. You should not join any groups which may be considered inappropriate and/or offensive to others.

13.22 Be aware that liking, sharing or retweeting can be viewed as an endorsement or a product, person or point of view.

13.23 Sensitive Personal Data as defined in the Data Protection Act 1998 or information classified PROTECT or above (as defined by the Government Protective Marking Scheme) must not, under any circumstances, be posted or disseminated on the internet and/or social networking sites.

13.24 Do not form inappropriate associations that may conflict with your role.

13.25 Do not reveal operational material or tactics on the internet or on social media.

14. LinkedIn

14.1 LinkedIn is a social media platform that is about building and engaging with the user's professional network. It is therefore acceptable for officers and staff to reveal that they work for the police, and in what capacity, on their personal LinkedIn site.

14.2 Notwithstanding this concession, all other terms and conditions of this policy must be observed.

14.3 Comments made by officers and staff on LinkedIn must always be professional, reflect the image of the Constabularies and not bring them into disrepute.

14.4 Information placed on LinkedIn remains within the public domain and is potentially accessible by those outside an individual's network.

14.5 There is a need to be cautious about 'endorsing' others on LinkedIn as the 'References' joint force policy has strict guidelines on the provision of employment and character references by officers and staff. Individuals endorsing others would effectively be providing a form of employment or character reference. In short, officers cannot provide a reference *at all* whereas staff can only provide one if their profile does not identify that they work for the police. Further guidance on this can be found within the 'References' Policy.