Altogether Better Policing

DURHAM CONSTABULARY POLICY

Durham Constabulary Freedom of Information Act Publication Scheme	
Name of Policy	**Standards of Professional behaviour on line**
Registry Reference No.	
Policy Owner	**Professional Standards and Legal Services Department**
Date approved at PUG	21.5.2020
Life Span	**3 years**
Version	1.0
Protective Marking	
Publication Scheme Y/N	
All Durham Constabulary policies are drafted in accordance with Human Rights and Equality Legislation	

Version Control

Version	Date	Reason for Change	Produced / Amended by
1.0			Victoria Fuller/Victoria Martin
2.0	21.5.2020	Reflect social media sites/use of and professional image	Victoria Martin/Faith Huntington

STATEMENT

The Police Standards of Professional Behaviour, Code of Ethics and Policing Principles all apply in the on line world as they do in the real world. Durham Constabulary must ensure that the conduct of employees on line does not have an adverse effect on their professional reputation, that of the force and public confidence in the police service. The Policy applies to any use of force systems and equipment both on-site and remote working (ref: NEP) and personal social media use.

The aims of this policy are to:

- Ensure that staff are aware of their responsibilities regarding the use of Durham Constabulary electronic **devices and systems**.
- Remind staff of the rules for **electronic communication**, including but not restricted to email.
- Inform employees who use the internet of their obligations, and what is deemed acceptable and unacceptable **internet use**.
- Outline the rules for **social media** use and to those who use dating sites in their private lives, providing guidance relating to on line personal safety.
- Explain the framework for the **access, monitoring and recording** of system use and electronic communications within the workplace.

This policy should be read in conjunction with the ***"Knowledge and information management policy"***, *and the "****Information security policy and procedures"*** (available on the intranet) which contains overarching guidance and additional detail related to information security.

Local and national anonymised examples will be provided for staff in text boxes to illustrate some of the points raised.

SCOPE

This policy applies to all Force personnel, i.e. police officers, police staff, police community support officers, special constables, volunteers, PCVC personnel, temporary staff, contractors/agency staff & apprentices.

Throughout this document the term "employee" will be used to refer to the above.

DEVICES AND SYSTEMS

Force systems and information must only be accessed from approved force equipment by authorised personnel and appropriately vetted individuals.

All force systems and information must only be used for a policing business purpose.

Employees must not search themselves on force systems (for example, incident logs, safeguarding reports etc) despite the personal data being about them, this includes information connected to themselves (for example, vehicles, locations, events etc). There are legitimate ways to obtain this and advice should be sought from the information rights and disclosure team. Employees must also not search for information relating to anything other than that required of a policing purpose (for example, associates, relations etc).

Any person found to breach this[1] could be liable to criminal prosecution under section 170 of the Data Protection Act 2018 (incorporating the General Data Protection Regulation), as well as internal disciplinary proceedings.

A member of police staff received a final written warning before a misconduct meeting for accessing police systems which was not for a legitimate policing purpose but out of personal curiosity.

Force systems provide access to confidential Force (and national) applications and therefore any security breaches affect the whole of UK policing and will be treated seriously.

Any suspected loss or compromise must be immediately reported to the Information Security & Assurance Manager and the IT service desk.

All passwords and access code authentication for force systems must be stored securely and must not be shared. Staff must not share passwords with colleagues or allow the use of systems by others using their log in. Staff should not use the same passwords at work that they use for personal accounts outside of the workplace.

External programmes, including those obtained via email, must not be downloaded onto Durham Constabulary's system or devices due to the risk of importing viruses.

Durham Constabulary allows the private use of Force owned mobile phones. However, employees using Force owned mobile phones for personal use do not have any expectation of privacy.

Users must sign up to the *Mobile Device Security Operating Procedures* before being issued with the device.

Durham Constabulary's mobile devices must not be taken abroad unless for work related purposes. Employees are reminded of the high cost of roaming and call charges in some countries. Furthermore, the encryption on the devices may be classed as illegal in some countries. Permission must therefore be sought from the Force Senior Information Risk Owner (SIRO) (Deputy Chief Constable) if the use of remote devices abroad is required. Please also refer to the *Mobile Device Security Operating Procedures*.

[1] including other directions throughout the policy

The use of force devices to access personal social media or dating sites is prohibited. Any use of social media and communication applications (i.e. Whatsapp) on force devices will be monitored.

The use of blue tooth on mobile devices is limited to certain operational roles and for hands free voice operation only. Access can be granted by the Information Security & Assurance Manager.

The use of the camera on mobile devices is permitted for operational use only. However, employees are reminded that mobile devices should not be used to record crime scenes unless as a last resort. They are not an adequate replacement for CSI quality images. If images do have to be captured via mobile device then it is the user's responsibility to ensure that they are suitably stored and adhere to the principles of evidential continuity and disclosure rules as well as the Data Protection Act and the Management of Police Information.

The use of body cameras is covered by the "*Body Camera Security Operating Procedures",* which users sign before issue of the device.

An officer resigned after being found to have been covertly recording colleagues using body worn video.

ELECTRONIC COMMUNICATION

Email

When used appropriately[2] email is a valuable means of communication amongst staff and with external parties. Unlawful or inappropriate use can infringe on the rights of others and can harm the reputation of the Force.

Staff are reminded to consider whether email is the best mode of communication in the circumstances and should ask themselves if off line conversation would be more appropriate.

Regular email (e.g. Hotmail / yahoo etc) is not secure as messages may be intercepted. Employees must therefore ensure that recipient's email addresses are secure enough to receive the information based on an assessment of it's of sensitivity and nature of the material being sent.

Employees should consider the content of the email and apply the appropriate government security classification (refer to the ***Information Security Policy and Procedures*** for further details). Only send the email to those who have a need to receive it, particularly when personal data is included.

[2] Use will be deemed appropriate if for a legitimate business purpose.

Employees must ensure that the recipient details are correct and double check before sending.

Securely marked material must only be disseminated via secure email addresses.

Employee personal email accounts must not be used for any force business. However, employees may email their own personal data, for example, pay slips, to themselves from their pnn.police.uk account.

A member of police staff received a written warning for emailing force information to their personal email account.

The force recognises that the majority of the information it now receives from members of the public, businesses & partners etc, is via email, which is often from insecure accounts. If an intended email reply contains sensitive information then this must be sent via alternative secure means. Any exception to this must be discussed with the Information Security and Assurance Manager.

Employees must not open attachments or click on links to websites from unknown sources and should contact the IT service desk for advice.

Employees must not use their @durham.pnn.police.uk account as a sender field when emailing content from the internet.

Work email addresses should only be used in order to conduct police business. They should only be used on sites that are directly linked to police business. For example, do not use your work email address on LinkedIn as this generates significant numbers of spam emails into the Constabulary.

Email must not be used to[3]:

- Conduct private/freelance business interests
- Conduct any private, personal &/or religious or political matters
- Engage in gambling
- Access/Disseminate pornography (except as part of a criminal investigation)
- Create/share chain letters
- Interfere with freedom of expression of others by jamming or bombing electronic mailboxes
- Enter into contractual commitments, unless advice has been sought
- Damage or otherwise interfere with Durham Constabulary systems or records which are accessible electronically

This list is not exhaustive.

[3] See also “unacceptable internet use”

Durham Constabulary will not tolerate messages that are:

- Offensive
- Illegal (e.g violation of copyright/data protection laws)
- Fraudulent
- Defamatory
- Derogatory
- Harassing
- Intimidating
- Obscene
- Disruptive
- Unethical

This list is not exhaustive.

The email system must not be used in instances requiring written authority under legislation. For example, PACE, warrants etc.

If staff are required to send an email on behalf of another then this must be made clear.

Instant messaging

Instant messaging (e.g. skype business) is a less formal approach than email. When employees work away from an office it can provide a valuable communication tool for colleagues and supervisors.

Instant messaging can be used for non-business purposes but this should be limited in nature and limited in terms of use in work time.

Two members of police staff were spoken to regarding the excessive use of the skype chat functionality when they were found to have sent thousands of personal instant messages.

Instant messages are recorded and stored within an archive which is accessible to authorised users within the Professional Standards Department. There should be no expectation of privacy.

Video Conferencing

Video conferencing (e.g. skype business, TEAMS) enhances modern methods of working/remote working. It provides a valuable communication tool for colleagues and supervisors. In addition it reduces the need for travel, when conferencing can be held

remotely. As with other force systems; Staffs are reminded that use is recorded, retained and is disclosable. Monitoring applies and there should be no expectation of privacy.

INTERNET USE

Internet access is available to all employees on networked terminals and via remote access. Subject to the principles and restrictions set out in this document, users will have access to a variety of websites and information. The internet must be used by employees in a sensible and appropriate manner both on and off duty.

Access to the internet via force systems for the following purposes is allowed on the understanding that the user conforms to policy at all times:

- To overtly access research material and information for a valid policing purpose relevant to an individual's role[4].
- Personal use (browsing) during recognised breaks or in a user's own time before or after work.

Internet use will be monitored and excessive use will be reported to the employee's line manager, which may result in access being removed and/or disciplinary action being taken.

Unacceptable internet use includes[5]:

- Creating, downloading or transmitting (other than for properly authorised and lawful research) data or other material or any data capable of being resolved into:
    - Obscene or indecent images
    - Defamatory, sexist, racist, offensive or otherwise unlawful images
    - Material designed to annoy, harass, bully, intimidate, inconvenience or cause needless anxiety to another person or
    - Material that infringes or breaches copyright or data protection.
- Publishing information known to be, or might be considered by others to be false, inaccurate, libellous, defamatory, pornographic, soliciting, vulgar, obscene, sexist, racist, homophobic, offensive or otherwise unlawful.
- Downloading/streaming video or audio for entertainment purposes &/or any unauthorised software. Advice should be sought from the IT department if in any doubt.
- Presenting personal views as those of Durham Constabulary.
- Spending excessive amounts of time browsing during work time.
- Making purchases. Use of Force systems is monitored and recorded, this essentially means that credit card details would be captured and potentially accessible by other staff.
- Subscribing to mailing lists which are not connected to police business.

[4] Different internet access may be given for different types of roles.
[5] See also email "don'ts"

- Knowingly do anything that is illegal under English law or the law of the relevant country.
- Accessing sites linked to dating, sex related sites and gambling sites.

This list is not exhaustive.

Any accidental or unintentional access to a prohibited internet site, or breach of the above, must be reported at the earliest opportunity to the Force IT and Professional Standards Departments via line management.

Violation of any of the above, inside or outside working hours, may be regarded as a disciplinary offence. In addition, the following are criminal offences under the Computer Misuse Act 1990[6] which may apply:

- ❖ Unauthorised access to computer material
- ❖ Unauthorised access with intent to commit or facilitate the commission of further offences
- ❖ Unauthorised modifications of computing material

SOCIAL MEDIA

Social media is defined here as being any on line channel which allows for the sharing of content between individuals or groups on line. This includes all social media services (list not exhaustive: for example: Twitter; Facebook; YouTube; Instagram; Flickr; WhatsApp; LinkedIn; on line chat forums and mobile only services).

Corporate accounts

Durham Constabulary recognises the benefits of corporate social media use:

- To engage with public & build rapport,

- To warn and inform, as well as gather information

- Reassure

- Increase visibility and accessibility of the police

Through the sharing of information on line.

Every communication produced by Durham Constabulary, or a representative of, is viewed by the public as official and can therefore impact positively or negatively on the reputation of the organisation and community confidence in the service.

[6] A relevant offence throughout the document

Any employee wishing to create a corporate social media account must liaise with the Media and Marketing Manager who will ensure that the request is in line with the Force social media strategy, approve the request and will maintain the administration of the account.

There is legislation governing information released to the public. Failure to comply with media law could result in contempt of court proceedings and compromise an ongoing investigation, amongst many other detrimental effects.

Staff using Force social media accounts are reminded:

- Durham Constabulary branding should be used on all corporate accounts.
- When posting about crimes individuals are only offenders once convicted, until then they are suspects.
- Suspects should not be identified by name until charged with an offence and a court appearance is imminent, i.e. the next day.
- Once proceedings are active i.e. arrests made, warrants executed, do not give too much information such as providing photographs and making comments.
- Victims of sexual offences have anonymity for LIFE. The public should not be able to identify the victim by piecing together other information released.
- Juveniles (Under 18s) cannot be named / identified even when they appear at court.
- Only the facts should be reported. Opinions and speculation should not be included. The person posting is responsible for checking the accuracy of the information. Once a post has been made public it is impossible to retrieve as it may have already been shared/screen shot.
- Advice should be sought from the media and marketing team regarding the release of photographs of convicted offenders.[7]
- Advice remains fluid and can change depending on prevailing circumstances. Therefore social media users are responsible for remaining up to date with the latest media guidance.
- Disparaging remarks made by the public on social media cannot be used as slander against the force as hosts of the page Durham Constabulary cannot be responsible for content posted by other people. However, if such remarks are detected then they should be brought to the attention of the media and marketing team, or an Inspector out of hours, to have it removed.
- Remain professional. Relatives of any individuals/incidents posted about are likely to be monitoring activity.
- Keep passwords safe and secure and notify Media and Marketing of any changes.
- Social media is a two way communication tool so be prepared to respond. If your post is in relation to a crime or incident then ensure that the appropriate mechanisms are in place for the comments to be reviewed, responded to and/or actioned.
- Although style should be conversational it must remain professional.

[7] Photographs of offenders will only be released if they receive more than 1 years imprisonment and were over 18 years of age at the time of the offence. Exceptions can be made if near to three years and it is deemed to be in the public interest.

- You must have the authority of the OIC/SIO to post about any crime investigation or incident.
- Operational tactics should NEVER be posted, nor should details which may undermine operational activity, such as live operation names.
- Information about internal processes, details which are confidential, sensitive, political or personal should not be posted.
- Posts must not be rude or aggressive or in any way likely to offend, including disparaging or defamatory remarks about the organisation, colleagues communities and partners.
- If a post is to reference a partner agency then prior permission should be sought from them.
- Durham Constabulary adopts the national guidance on the release of images of unknown suspects / witnesses that police would like to trace and speak to. Approval must be confirmed in writing by the OIC or SIO to ensure that the required conditions are met:
    - Guilt must not be implied and the wording must be approved by an Inspector or above,
    - must not include any other person,
    - must be of sufficient quality,
    - no other investigation would be compromised,
    - the image has been circulated internally,
    - the CCTV owner has agreed to the publication,
    - the release of the image is proportionate.

Ensure that there are adequate plans in place to monitor any social media replies. The Professional Standards Department must be informed by the person tasked to monitor the post if any reply constitutes a potential complaint against police.

Personal use of social media

Everyone is entitled to a private life but employees must ensure that their personal use of social media doesn't discredit themselves or the force, either on or off duty. Standards of professional behaviour apply as much on line as they do off line.

An officer received a written warning after asking a member of the public to be their friend on Facebook during a house visit.
A member of police staff resigned over excessive and inappropriate use of social media during working hours.

Employees are reminded that:

- They should not use their own personal social media account whilst on duty in a public area.
- In order to protect staff personally (and their vetting status), their family and friends - employees should have careful consideration before making any reference to Durham Constabulary or the work it conducts. It could present a personal security risk or an operational risk.
- Employees taking photographs/selfies in the work environment should be aware of their environment to ensure that unsuspecting colleagues or information on screens/walls/desks is not viewable.
- They are accountable for whatever is posted on their personal site. All comments on social media are deemed to be in the public domain.
- The media, criminals and the wider public use social media platforms to gather information regarding Constabulary employees.
- Employees are reminded that they should not share compromising/sensitive information or photographs via any social network platform as it leaves them vulnerable to corruption e.g. sharing of naked 'selfies' via dating apps.
- Employees must not express personal views which may be derogatory towards colleagues, Durham Constabulary policies/procedures/operations and activities nor those of partners.
- Employees must not provide information about a crime or incident or other Durham Constabulary related matter via their personal social media account. The Durham Constabulary official account should be the official source of the information.
- They must comply with data protection rules in the same way as they should elsewhere on and off line. Maintain confidentiality.
- Strong language, capital letters and exclamation marks can be easily misinterpreted on line in the absence of body language and tone of voice.
- Sarcasm and humour should be used with care.
- Nothing is ever truly private on line but employees should ensure that they know their privacy settings.
- It is important to verify the identity of friend and group requests before accepting them. If in doubt, decline.
- Social media content should reflect the Code of Ethics and the values of Durham Constabulary so as not to damage the reputation of the individual and/or organisation.
- Employees must not use a force system to access personal social media &/or dating accounts.
- Employees should not use public wifi in Constabulary premises to access dating, sex or gambling sites.

Overarching advice

All employees should consider what they send electronically, both at work and of duty. All staff have the right to privacy and free speech however this has to be balanced against what

is acceptable under the Standards of Professional Behaviour and the potential to bring discredit on the police service as a whole. In any electronic communication, whether encrypted or not, on or off duty – individuals should apply the test as to whether the comments, content or material would be considered appropriate in the workplace and in line with the Code of Ethics and the Standards of Professional Behaviour before sharing or sending any material.

It is recognised that technology develops at a fast pace and this policy may not cover every device or all software in the long term. The guidance will relate to other smart devices alongside those mentioned e.g. smart watches.

The Standards of Professional Behaviour include a specific reference to ***Challenging and reporting improper behaviour.*** This essentially means that as well as being responsible for their own behaviour, if employees witness or are aware of the inappropriate conduct including the use of electronic devices or inappropriate communication – they have a positive duty to report, take action or challenge. Failure to act can in itself result in a breach of the Standards of Professional Behaviour.

EQUALITY IMPACT ASSESSMENT (EIA)

Title
An equality impact assessment (EIA) form **must** be completed by when developing or reviewing policies or procedures or introducing a new scheme which may impact on the way the Force conducts its business (both internally and externally) and must show that when making decisions we:- • Give due regard to the impact it will have on protected groups • Undertake an assessment **prior to** any decisions around policies/procedures being ratified to identify what potential impact has been found and subsequent action taken, and • Provide an audit trail of the assessment undertaken which identifies how the policy or procedure is likely to affect protected groups. The EIA must be completed **before** decisions are made, and remain a live document to be reviewed and continually updated during policy/procedure development or updating This form is a Tool to document the assessment and should be completed, attached to the relevant policy/procedure document and submitted to the relevant strategic group for ratification
1) Purpose of the Policy/Procedure/Scheme. Why do we need it and what will it achieve
The policy is intended to provide staff with clear guidelines regarding what is expected of them when using for electronic systems. It also advises them regarding electronic communication both in and outside the workplace.
2) What research/resources have been used or considered in the initial stages of this assessment?

I have taken specialist advice from the force information department to ensure that advice was current and legal. Discussions took place regarding any negative impact on specific groups and none was identified. Staff associations have not raised any issues with this policy.

3) Explain briefly why the Policy/Procedure/Scheme is being developed or reviewed?

The policy was required as existing policies did not cater for online behaviour. Also technology is changing so fast, and in particular methods of communication that the policy is required to protect the public, staff and the organisation.

4) Who has been consulted around the potential impact during the development/amendment of the Policy/Procedure/Scheme

All support networks.	Force Executive (AC0)
HR Staff	Independent Advisory Groups (IAG's)
Staff associations	Legal Services
Heads of Command	Ch Supt Curtis

5) Following assessment of available information, has a positive or adverse impact been identified OR is the initiative equality neutral?

A **Positive Impact** – will actively promote equality of opportunity or improve relations between one or more groups

An **Adverse impact** – will cause some form of disadvantage or exclusion.

Neutral impact is when there are no notable consequences for any diversity group

Provide details on ALL decisions for ALL the protected characteristic groups below. Specify what actions, if any, will be taken as a result of the assessment, provide any findings and the reason any decisions were reached, and determine what changes may be necessary to either reduce any adverse impact or enhance any beneficial impact.

If an adverse (negative) impact has been identified question 5 must be completed.

	Positive	Negative	Neutral	Details
Age			X	
Disability			X	
Transitioning from one sex to another (either thinking of, in the process of or have)			X	
Marriage and Civil Partnership			X	
Pregnancy and Maternity			X	
Race			X	
Religion or Faith			X	
Gender			X	
Sexual Orientation			X	

6) If a negative impact has been identified, please provide further details stating what actions need to be undertaken as a result of the section 4). How any negative impact can be justified for this initiative.

Confirm the above Actions have been incorporated and the EIA is now ready for submission to relevant Strategic Group.

Signature… V. Martin

Name Victoria Martin **Date** 21.5.2020

7) – Ratify the Policy / Procedure at relevant Strategic Group
Meeting/Group:- Policy User Group 21.5.2020
Chair of Meeting/Group:- Ch Supt C Curtis.