# POLICE AND CRIME COMMISSIONER FOR LEICESTERSHIRE

# ETHICS, INTEGRITY AND COMPLAINTS COMMITTEE

PAPER MARKED

C

| | |
|---|---|
| Report of | **DEPUTY CHIEF CONSTABLE** |
| Subject | **LEICESTERSHIRE POLICE CYBER BEAT** |
| Date | **FRIDAY 24 JUNE 2016 – 2:00 p.m.** |
| Author | **SUPERINTENDENT M MULQUEEN** |

## Purpose of Report

1. The purpose of this report is to make the committee aware of Cyber Beat, a new initiative to be piloted later this year, by which the techniques of neighbourhood policing will be exercised using freely available social media platforms.

## Recommendation

2. It is recommended that members discuss the proposal voicing a view of its ethics and integrity from a community perspective.

## Background

3. As a service we have, traditionally, operated an approach to neighbourhood policing (NHP), well recognised in Great Britain, whereby police officers have striven to connect to the public in general and more specifically with otherwise hard-to-reach individuals, including vulnerable individuals. Central to the approach is police being physically present among the public. It is an approach designed to build trust and relationships via association rather than through crime-focussed policing transactions alone. However, rapid and socially influential developments in digital technology challenge this approach. These developments juxtapose person-to-person neighbourhood policing with the task of reaching into the lives of individuals whose social, financial and educational existences are being routinely conducted in the virtual space of the Internet. Furthermore, ongoing austerity in UK public service provision places pressure on the budgetary capacity of policing organisations, including Leicestershire Police, to resource a substantial physical presence of neighbourhood policing in the community. In a practical and straightforward way Cyber Beat is an attempt to help address these challenges of digitalisation and finance.

## How it is Intended to Work

4. The project team intends to run a pilot Cyber Beat between September and December 2015. Piloting will comprise use by police officers and PCSOs of familiar, free and generally available social media platforms (e.g. Facebook, Instagram) to conduct the varied techniques of on-street NHP including informal real-time chat, welfare checks, and safety awareness promotion. It will operate along two strands: one strand will see Cyber Beat promoted to elderly users where the intended effects will be *inter alia* increased contact (even companionship) between police and elderly people; increased consumption of advice on personal safety and well-being among elderly users in the community; an enhanced sense of personal security/safety among users, and better targeted welfare checks by officers. Regular, agreed (e.g. once weekly) check-ins by police on elderly people both offer a social outlet to those we might otherwise engage with less often and, critically, activate welfare calls to the person's home that might not otherwise occur. The second strand will be an attempt to reach out to young people in more controlled communities within Leicester's diverse demography. The intended effects will be *inter alia* building positive relationships based upon trust with vulnerable young people; an increased sense of user security and safety against problems often associated with controlling communities, including radicalisation and honour based violence (HBV); better awareness among users of online safety. As such the service will seek to engage in more meaningful ways with those whose lives are routinely played out on the digital street. Secondly, Cyber Beat will provide to such people a means of communication with the police that may seem more 'normal' and discreet than engagement with officers on the physical street.

## Ethically Focussed Preparation

5. The Cyber Beat project leadership team comprises Superintendent Mark Newcombe, Superintendent Michael Mulqueen and Chief Inspector Lou Cordiner. The team is committed to ensuring the project is underpinned by, and operated entirely in accordance with, a rigorous framework of digital ethics. During the early development phase Supt Newcombe and C/I Cordiner are responsible for strategic and operational delivery of the pilot while Superintendent Mulqueen is responsible for design of the ethical framework, ethical leadership and implementation. Among his relevant publications is his latest (June 2016, Palgrave Macmillan) co-edited book on Big Data ethics. Previously, as Full Professor of Media and Security Innovation at Liverpool Hope University, he served as the NPCC's academic expert on innovation and ethics in Digital Intelligence and Investigation, under Chief Constable Stephen Kavanagh. He held various senior university appointments including professorial member of the Ethics Committee; as such he held high-level responsibility for ensuring that all staff and student research was in compliance with the Universities UK Concordat to Support Research Integrity. Mulqueen is conducting the Cyber Beat pilot in fulfilment of an action research project assessment, which has been set for superintendents entering the service under the Direct Entry Scheme. As such, the project has already come before the Research Ethics Committee of Teeside University, which, in a direct collaboration arrangement with the College of Policing, is awarding postgraduate diplomas to those who successfully complete the DE scheme. The Teeside ethics committee passed the project without modification. While, therefore, the project, as envisaged, clearly meets with UK standards for integrity in research ethics, the project team, nevertheless,

invites the observations of the Leicestershire ethics committee to help enrich Cyber Beat's ethical foundations.

## Ethical Challenges

6. The ethical framework being developed to support Cyber Beat has so far identified a range of challenges against which the emerging design and implementation of the project need to be evaluated. Several such challenges are summarised below:

Consent:

- Users need to be fully informed that police may need to act on information that s/he may impart on Cyber Beat, which will be staffed by personnel who are professionally bound to uphold the law and safeguard the community. Clear and straightforward messaging highlighting police responsibilities with information is therefore critical to the user.
- Users must not feel pressurised to respond to police requests for engagement. In clear language the community must be assured that no negative implications arise to them by choosing not to cooperate with police through Cyber Beat.

Safety:

- Engaging with the police at any time, on the street or online, can be dangerous for people in certain vulnerable situations. Easily accessible, current safety advice and routes through to our wider policing services are therefore essential. This point is further elaborated, below, under Risk/Impact.
- To protect users and victims the Cyber Beat team must resort, where necessary, to the content moderation tools provided by social media platforms.

Digital/Non-Digital Equality:

- Improvements in the services we offer to digital users must be accompanied, wherever reasonable, by improvements in services to non-digital users. Users need to be trained if possible in several social media platforms on which we can communicate.

Intelligence boundaries:

- Cyber Beat will not operate as an intelligence tool *per se* nor be subject to surveillance authorisations.

Well supported staff:

- While many staff know how to use social media platforms good training is necessary to promote deeper understanding of policing challenges on social media, e.g. privacy. Equally the service must effectively support, supervise and manage those personnel.

## Currently Ethically-Focussed Actions

7. Proactive engagement with these challenges is underway. This summer, Cyber Beat's ethical challenges are being evaluated for a research paper and mapped into a subsequent user handbook. Potential staff and trainers (e.g. initial crisis negotiation online) are being identified. By way of locating ethical and other improvements after the Cyber Beat pilot – should the service wish to proceed beyond pilot - the project team is engaging with colleagues at Nottingham Trent University (NTU), under the aegis of the East Midlands Police Academic Collaboration (EMPAC), to evaluate successful attainment of the pilot's outcomes.

**Implications:**

**Financial:** Staffing and equipment costs for the pilot are set out below. Costings are prepared on the basis of three months deployment undertaken by a PC and PCSO. It may be, however, that the most qualified individuals have attained higher rank and so costings will need to be adjusted accordingly.

| | Average 3 month Cost with on costs |
|---|---|
| PCSO (includes 14% Shift Pay) | £7,406 |
| PC (Joined before Apr-13) | £10,587 |
| PC (joined after Apr-13) | £8,942 |

| | | |
|---|---|---|
| Laptop x 2 | £677 (£1,354) | |
| BlackBerry x 2 | £25 (£50) | |
| BlackBerry rental x 2 x 3mths | £17.50 (£35) (£105) | |

**Legal:** It has been recognised at the project initiation stage that interaction with members of our communities via the Cyber Beat pilot may involve the processing of personal information, although the pilot will not set out to deliberately capture new data, but focus upon open source publically accessible social media platforms to enable interaction. It is recognised there may be low level privacy issues identified that could require assessment and mitigation.

The legislative framework around the processing of personal information is the Data Protection Act 1998, the obligations of which are further enhanced within the police service by adherence to a statutory Code of Practice entitled the Management of Police Information (MoPI) 2005. In recognition of this full and early engagement with the Information Management Section within Leicestershire Police has formed a central piece of governance for the pilot.

There will be emphasis within the pilot on the processing of personal data through the use of consent in that members of the communities will be agreeing to engage with the police using social media. To further ensure the ethical and transparent usage of personal data within the pilot it is intended to consider a Privacy Impact Assessment (or PIA), as championed by the Information Commissioner's Office (ICO). The PIA will assist us to:

- Identify any privacy risks to individuals.
- Identify any privacy liabilities for Leicestershire Police.
- Enhance public trust and confidence through ethical and transparent use.
- Protect Leicestershire Police reputation.

**Risks/Impact:** The project team identifies a risk of harm arising to people who live in coercive environments and who are found to be using Cyber Beat by those who are exerting harm, as the risk of highest potential impact arising from the project. Especially at pilot stage the likelihood of the risk occurring is considered low. In the absence of Cyber Beat such victims may not have any other means to engage directly with the police to provide safeguarding measures to them. When they do engage via Cyber Beat, and, indeed, in any instance where a conventional policing response may be more appropriate, the Cyber Beat team will operate to a protocol whereby victims will be supported and encouraged to access our services through existing modes of contact in the first instance (rather than using openly readable social media platforms). Victims or those wishing to report crime will therefore be directed towards direct/private messaging, 101, email, face-to-face contact or text message. Where officers believe on the basis of their dynamic risk assessment that they should alert the appropriate (e.g. specialist) teams, they will be supported in so doing. The protocol will, consequently, ensure that any identified demand will be managed into the correct existing mechanisms. It follows that that the pilot team will not be overwhelmed with such demand.

Due to overt and public nature of this pilot using social media platforms, it is not anticipated that the volume of such disclosure will be high. However this will be formally assessed in an evaluation of the pilot, to be conducted by researchers from Nottingham Trent University, acting under the aegis of the East Midlands Police Academic Collaboration (EMPAC).

**Equality Impact Assessment:** An Equality Impact Assessment (EIA) of the project has resulted in the project team identifying measures to mitigate digital inequality arising in the delivery of Leicestershire Police services. Lack of Internet access and lack of skills in the use of the freely available social media platforms that Cyber Beat will utilise are considered the primary drivers of inequality that may arise from the initiative. This may apply, in particular, to older people although not exclusively so. Consequently, Cyber Beat has included within the set of ethical principles on which it will operate the following: that which we deliver digitally should also be delivered non-digitally, whenever it is reasonable to do so. Reduction of inequality should be achieved by greater attentiveness to neighbourhood contacts with older people who do not use digital means and by providing social media training in the community.

**Link to Police and Crime Plan:** In June 2016, Leicestershire PCC Lord Bach set out a number of priorities for policing, of which the top three were:

1. More visiting Neighbourhood Policing on the streets:
2. Greater effort against hidden crimes: hate crime, domestic violence, and cybercrime.
3. Greater engagement with the public

Cyber Beat explicitly recognises that more people are spending more of their lives on the digital street. Cyber Beat fills a gap in our capability to provide neighbourhood policing that is better tuned to both the virtual and physical lives of the people in the communities we serve.

Clearly, the capacity to reach out discreetly to the police is important to victims of hidden crimes including domestic violence, honour based violence, forced marriage, and Female Genital Mutilation (FGM). Cyber Beat provides a mechanism by which we, as a digitally-enabled service, can foster and nourish relationships that strengthen community resilience against such practices. Additionally, Cyber Beat, by moving us centrally into the operating space of digital users brings us closer to those vulnerable to cybercrime. As such, we are better positioned to encourage practices that help prevent cybercrime (e.g. good Internet hygiene) and, where it occurs, to encourage timely reporting of cybercrime as an aid to investigation.

Whereas the PCC rightly encourages greater public-police engagement our neighbourhood policing service, as currently calibrated, does not employ in a widespread way freely available, popular social media platforms to reach into the digital lives of individuals in the community we serve. We are, as such, unavailable to those whose lives are routinely and substantially conducted on social media. Furthermore, we are missing an opportunity to harness better contact with those who may not routinely use social media but by it can enjoy greater contact with police than resources might otherwise allow.

In these key respects, therefore, Cyber Beat readily aligns with the PCC's priorities.

**Communications:** A communications plan will be developed to support the CyberBeat pilot project and identify any reputational and media risks associated with 'engaging in the community's conversations'. The plan will consider the following points:

- Understanding the community
  - Audience profiling, interests and platforms used, targeting and how we reach the audience, digital channel selection (eg social media, skype, blogs, polls, etc), the different needs and requirements for each channel, identification of partners/stakeholders and learning from other forces (eg Derbyshire Digital PCSO)
- Trusted source of information
  - Establish whether it is the 'police' that is the trusted source for credible information or whether this is a barrier to communication and identify partners and 'Peer' influencers on digital channels that can disseminate information on behalf of the police
  - Content must be closely linked with wider communications strategy delivered by Communications and Engagement Directorate
- Tone of voice
  - Training to develop consistent tone of voice and develop the 'personality' for each channel framing content appropriately based on the digital channel selection
- Moral/ethical
  - Identify the processes in place to safeguard victims when disclosures are made or process crimes when reported
  - Measures – what are the measures of success? Engagement, reach, confidence and satisfaction, repeat contact etc.
- Risks:
  - The rate of technological adoption, accessibility to internet and use digital channels which may impact service adoption
  - How to react to backlash and the audience reacting negatively to the police being in their virtual world or entering into gated communities
  - Channel management and responses and a recognition that there is more than 'social media' in digital communications, so the police will need to consider these additional channels eg blogs, video conferencing etc
  - Training - digital comms training and governance linked to force social media policy
  - Although some social media channels have a private conversation function, it must be remembered that these channels are open comms platforms and therefore not private or safe places
  - The naming of individual officers online to create and build community relationships may place officers/PCSOs at risk
  - Managing negative posts and 'trolling' activity
  - Governance, training and guidance for the pilot will be from the Digital Media Team and will be linked to force social media policy

**<u>List of Appendices</u>**

None.

**Background Papers**
None.

**Persons to Contact**
Superintendent M Mulqueen
Tel: 0116 248 5675, email: michael.mulqueen@leicestershire.pnn.police.uk

Superintendent M Newcombe
Tel: 0116 248 3339, email mark.newcombe@leicestershire.pnn.police.uk