Information Compliance and Records Management Unit (ICRMU)
Information Management Branch

Date: 26/07/2023
Our ref: 01/FOI/23/002513/B

FREEDOM OF INFORMATION REQUEST REFERENCE NO: 01/FOI/23/002513/B

I write in connection with your request for information dated 26/06/2023, received by Greater Manchester Police (GMP) for the following information:

I respectfully request a reply in relation to all the policies I have requested; please provide a reply in relation to my request for the following policies:-

1. GMP Policy guidance on recognising cyberstalking and cybercrime. How does GMP provide training to officers to recognise cyberstalking and cybercrime?
2. GMP policy documents on online hate crime
3. GMP policy documents on cyberstalking and cybercrime

Result of Searches
Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate information relevant to your request. I can confirm that the information you have requested is held by GMP. However, I am not obliged to supply you with all the information held as exemptions apply.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because this information is exempt) to provide you, the applicant, with a notice which: (a) states that fact, (b) specifies the exemption in question and (c) states (if that would not otherwise be apparent) why the exemption applies. Where redactions in the attached Policy & Procedure documents have been made, that information is exempt from disclosure by virtue of the following exemptions: **Section 40(2)(a) – Personal Information, Section 31(1)(a)(b) – Law Enforcement** and **Section S21 – Information Accessible to Applicant by Other Means.**

Where **Section 40** has been used, this represents information that identifies a living individual, to disclose this information would breach the principles of the GDPR and the Data Protection Act 2018. Personal data is defined by Article 4 of the GDPR and Part 1 of the Data Protection Act 2018, and means any information relating to an identified or identifiable natural person ('data subject'). An identified natural person is one who can be identified directly or indirectly from that data.

Section 31 is a qualified and prejudice-based exemption and as such, subject to a harm and public interest test.

Evidence of Harm

To provide the redacted information within the attached policy would reveal policing tactics used by Greater Manchester Police. This would give an advantage to that are intent on committing offences and avoid detection. It would also increase the risk of danger towards the public GMP who sworn to protect.

Public Interest Test

Factors Favouring Disclosure

To disclose the redacted information would provide the public with a slightly more in-depth knowledge into how Greater Manchester Police operates. This would enable the populace to take steps to protect themselves against criminal activity and may lead to further information being provided to the force.

Factors Favouring Non-Disclosure

Conversely to the factors in favour of disclosure, to release the redacted information into the public domain would reveal the policing tactics of Greater Manchester Police. This would impact on the force's ability to detect and prevent crime and apprehend and prosecute offenders. The risk of danger to the public would be increased by revealing such policing tactics into the public domain. The safety of the public we protect is of paramount importance to Greater Manchester Police and we would not wish to jeopardise that safety by releasing exempt information into the public domain.

Balancing Test

The arguments for and against disclosure of information need to be weighed against each other. In this case the greatest argument for disclosure is the fact that the populace would be provided with information regarding how the force police operate. However, given that the disclosure would increase the risk of increased crime to and assist those intent on committing crime to avoid detection the balance of disclosure, at this time, weighs on non-disclosure for those redacted parts of the policy requested.

This letter acts as a refusal notice for the redacted parts of the attached Policy and Procedure documents.

Regarding the training element of your first question, this information is exempt under **Section 31(1)(a) – Law Enforcement.**

Evidence of Harm

Disclosure of the information on training courses for Police Officers could be of intelligence value to a person or persons with criminal or malicious intent. The disclosure could provide and enable targeted malicious actions, be that some form of attack on an operational team or officer or avoiding that team for example where strengths and weakness may be perceived (whether incorrectly or not). Providing details of training provides opportunities for criminality to benefit, or for risks to be extended to members of the public.

Public Interest Test

Factors favouring disclosure

Providing this information would make members of the public more aware of the level of training Police Officers receive to members of the public against cybercrimes and stalking activities.

Factors favouring non-disclosure

The Police Service exists to protect and serve the public through the prevention and detection of crime. To provide such information at force level, it could compromise law enforcement tactics which would hinder the Police force's ability to detect and successfully investigate cybercrime, including cyberstalking. The threat of crimes will increase as more crimes are committed as a result of criminals gaining knowledge about the capabilities of the forces. Therefore, the public will be placed at a greater risk. A fear of crime will be realised as criminals identify different levels of training regarding different officers and target and exploit this resulting in the public being in fear of more criminal activity occurring. The safety of the public is of paramount importance to Greater Manchester Police and to release the requested information would compromise the safety of the community that Greater Manchester Police serve to protect and place individuals at risk.

Balancing test

When balancing the public interest Greater Manchester Police must consider whether the information should be released into the public domain. Arguments need to be weighed against each other. The most persuasive reason for disclosing the information would be openness. However, this needs to be weighed against the strongest reason for non-disclosure which is the fact that individuals may be placed at risk and the affect it may have on the prevention and detection of crime and protecting the people and communities we serve.

This letter acts as a refusal notice for the training element of question one.

The Hate Crime Policy and Procedure can be found here.

The Fraud Recording, Screening Allocation and Investigation Procedure can be found here.

The Stalking and Harassment Policy and Procedure can be found in a response to a previous Freedom of Information request here.

Please find attached a redacted copy of the Internet Based Research and Investigation Procedure.

Internet Based Research and Investigation

Procedure

Greater Manchester Police

[April 2014]

PROCEDURE IMPLEMENTED: April 2014

REVIEW DATE: April 2017

PROCEDURE OWNER: Force Intelligence Bureau, Covert Section

APPROVED BY: [redacted] (Force Cybercrime Lead)

PROTECTIVE MARKING: Restricted

IS THE PROCEDURE ☑ New ☐ Revised

IF REVISED, PLEASE COMPLETE TABLE BELOW

VERSION NO	DATE	SUMMARY OF CHANGES	AUTHOR(S)
1.0	April 2014	First version of procedure published	[redacted]
1.1	May 2014	Updated section 3 with list of NCALT e-learning packages as per College of Policing cybercrime APP web page update (6th May)	[redacted]

Table of Contents

1. Introduction and Background

The use of the internet and social media is constantly evolving. This procedure will ensure that Greater Manchester Police adheres to current legislation whilst conducting effective and proportionate online research and investigation.

The collection of information for a policing purpose from the internet has increased significantly recently and clarity is required as to what activity may require authorisation under Regulation of Investigatory Powers Act 2000 (RIPA) or the specialist assistance of a Covert Internet Investigator (CII).

The purpose of this document is to outline the procedures in relation to such activity.

2. Scope

This document details procedures that adhere to current Association of Chief Police Officers (ACPO) Guidelines, Human Rights Legislation and the Regulation of Investigatory Powers Act 2000 (RIPA) that must be followed when conducting online research and investigation.

This procedure provides minimum standards that must be adopted by all persons engaged in open source internet research and investigations in order to maintain the integrity of any evidence gained and in order to avoid compromise of the following:

- The hardware/software infrastructure of police computer systems;
- Police tactics;
- Ongoing and future police operations;
- The personal safety of individuals;
- Reputational risks to the organisation.

It is not the intention of this procedure to prevent members of staff conducting routine searches as part of their daily business. For example, the searching of a telephone number on 'Google' before submitting a Focus 112 application for subscriber details.

However, once the initial search has led to a website/ forum/ business, staff should cease any conduct unless they have attended the Mainstreaming Cybercrime Training (or other approved/ accredited) Course, to prevent a footprint being left on sites that have tools to grab the Internet Protocol (IP) addresses of persons visiting.

Research must be truly open source and comply with the Appropriate Use of Electronic Communications and Information Systems Procedure. Even though this searching maybe for a specific operation, it is not considered to be covert or likely to obtain private information. The data returned is likely to be publicly available.

3. Roles & Responsibilities

The Force Authorising Officer (AO) believes there has to be a pragmatic approach, when open source research is being undertaken in the course of our daily business to obtain intelligence and evidence to support criminal investigations.

The purpose of this document is to outline the procedures in relation to this activity. All members of Greater Manchester Police must adhere to these procedures when undertaking open source research.

The following NCALT e-learning packages are available to assist in understanding of the issues involved:

1. Communications data and cyber crime – introduction to law and procedure
2. Communications data in investigations
3. Communications data – introduction to the internet
4. Cyber crime and digital policing – first responder
5. Cyber crime and digital policing – introduction
6. Cyber crime and digital policing – investigation
7. Digital communications, social media, cyber crime and policing
8. Introduction to communications data and cyber crime.

4. Terms and Definitions

The primary aim of Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) was to comply with the “legality” requirement of Article 8 of the European Convention on Human Rights which provides a right to respect for one's "private and family life by providing a lawful framework for police surveillance activity.

4.1 Directed surveillance

This can be summarised as meaning surveillance which is covert, conducted in such a manner as is likely to result in the obtaining of private information about a person, for the purposes of a specific investigation or operation and otherwise than as an immediate response to events (*RIPA, Section 26(2))*

In determining whether surveillance of public internet sites and Social Networking Service (SNS) profiles requires a RIPA authorisation we need to look at the definition.

4.1.1 Surveillance

This is defined as the monitoring, observing, listening to persons, their movements, their conversations or their other activities or communications; Recording anything monitored, observed or listened to in the course of surveillance, and surveillance by or with the assistance of a surveillance device. Surveillance is watching rather than seeing, listening rather than hearing. (*RIPA, Section 48(2))*

4.1.2 Covert surveillance

The second criteria of the definition of directed surveillance is that it must be covert. Surveillance is covert “if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that surveillance is or may be taking place”. *(RIPA, Section 26(9)(a))*

4.2 Private information

In relation to private information, since information on the internet and open SNS profiles is public, such surveillance might be expected to fall outside the definition.

However, RIPA defines "private information" broadly and the Covert Surveillance and Property Interference Revised Code of Practice clearly supports this interpretation stating:

"The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis".

4.2.1 Code of Practice example

"Two people holding a conversation in the street or on a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information"

The Office of Surveillance Commissioners Procedures and Guidance 2011, (at 308.1) states: "Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed to be published and no longer under the control of the author, it is unwise to regard it as 'open source' or 'publicly available".

Expectations of privacy can still persist when there is a recording, retention and systematic storage of information that provides a profile.

In the case of Rotaru v Romania the European Court of Human Rights observed how, "Public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."

Regular and frequent reviewing of Open Source information that has been published about a living person may lead to the activity being considered as likely to obtain private information. Frequently accessing open source information needs to be kept under constant review in case private information is being obtained.

4.3 Open source research

"The collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise to use as intelligence or evidence within investigations" *ACPO Online Research and Investigation Guidance*

4.4 Open source information

"Publicly available information (i.e. any member of the public could lawfully obtain the information by request or observation). It includes books, newspapers, journals, TV and radio broadcasts, newswires, Internet WWW and newsgroups, mapping, imagery, photographs, commercial subscription databases and grey literature (conference proceedings and institute reports)"
ACPO Online Research and Investigation Guidance

For the purposes of this procedure it is recognised that commercial subscription databases may contain some data not available to the public but within the terms of the procedure they are still considered open source.

5. Procedure

ACPO promotes five levels of internet investigation/ research. However Greater Manchester Police and the North West Counter Terrorism Unit have consolidated these into three levels which are outlined below.

The criteria detailed in the following standards should be seen as the minimum standard when carrying out operational activity on the internet. Units should assess their operational requirements individually and set operational criteria accordingly as long as it does not fall below the minimum standard.

[redacted]

[redacted]

[redacted]

6. Associated Documents

Prior to engaging in any open source investigation/ research staff should have a good understanding of the Legislation and Guidance that may apply.

- ACPO Online Research and Investigation Guidance
- ACPO Good Practice Guide for Digital Evidence
- Human Rights Act 1998 (HRA)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Computer Misuse Act 1990 (CMA)
- Data Protection Act 1998 (DPA)
- Police and Criminal Evidence Act 1984 (PACE)
- Criminal Procedure and Investigations Act 1996 (CPIA)
- Police Act 1997
- Authorised Professional Practice – Information Management (this has superseded the MoPI Guidance)

7. Consultation & Statutory Compliance

7.1 Consultation

Department	Comments
North West Counter Terrorism Unit (NWCTU)	Consultation undertaken to ensure that GMP's procedure acknowledge the good practice established within NWCTU procedures

7.2 Statutory compliance

7.2.1 Data Protection Act (1998)

This procedure aims to support Greater Manchester Police Officers in conducting research and investigation online. Such activity may well involve the processing of personal information and, as such, in developing the procedure, close attention has been paid to the Data Protection Act, as well as other associated legislation and guidance including the Regulation of Investigatory Powers (RIPA) Act 2000 and the Office of Surveillance Commissioners Procedures and Guidance 2011.

Any personal information that is processed as a result of internet based research and investigation should be done so in accordance with the force's Data Protection Policy. Personal data that is obtained and held by the force following internet based research and investigation carries an inherent sensitivity and therefore must be stored, handled and disposed of in accordance with the force Government Protective Marking Scheme Procedure to ensure it is afforded the necessary safeguards to prevent unauthorised access and accidental loss, damage or destruction.

7.2.2 Freedom of Information Act (2000)

This procedure has been classified as 'RESTRICTED' under the Government Protective Marking Scheme and therefore should it be requested under the Freedom of Information Act 2000 please contact the Information Compliance and Records Management Unit [redacted] so that it can be assessed for disclosure/exemption.

7.2.3 Equality Act 2010

This procedure will not have any effect on equality for any of the protected characteristics considered within current equality legislation. Online research and investigation will used (and where necessary, authorised in accordance with legislative requirements) as a tactic against persons irrespective of their age, race, gender, religion etc.

Moreover, introducing the 'Internet Based Research and Investigation Procedure' will benefit the quality and effectiveness of the service GMP provides to our diverse communities and people covered by protected characteristics under equality legislation. Whilst anyone can become a victim of cybercrime, there are ways in which cybercrime can affect people or communities that share a protected equality characteristic. For example, people may find themselves a victim of cybercrime linked to their ethnicity, religion, or sexual orientation (e.g. hate crime conducted through social media), young people can find themselves victims of cyberbullying, or older people may find themselves the target of financial cybercrime.

8. Appendices

No appendices