



[REDACTED]

Date: 16/05/2023
Our ref: 1874/23

[REDACTED]

FREEDOM OF INFORMATION REQUEST REFERENCE NO: GSA 1874/23

I write in connection with your request for information dated 11/04/2023, received by Greater Manchester Police (GMP) for the following information:

- 1. How many police officers are currently assigned to Local Policing Teams and Community Policing Teams in Greater Manchester Police as of 8th April 2023?*
- 2. How many police officers and staff in Greater Manchester Police are currently issued with a Smartphone as part of their official duties as of 8th April 2023?*
- 3. Can you able provide a breakdown of what departments and teams are issued with smartphones and who are provided with Android and/or Apple devices and tablets?*
- 4. How many police officers and staff in Greater Manchester Police are issued with Android Devices or tablets as part of their official duties as of 8th April 2023?*
- 5. How many police officers and staff in Greater Manchester Police are issued with Apple Device or tablets as part of their official duties as of 8th April 2023?*
- 6. What accessibility requirements, if any, do police-issued smartphone applications conform to, such as the Web Content Accessibility Guidelines (WCAG) or other standards, to ensure that the app is usable by as many people as possible, including those with disabilities?*
- 7. What measures are in place to ensure that police officers and staff with disabilities are provided with appropriate accommodations, including accessible devices and applications, to perform their official duties effectively?*

8. Do police officers and staff deployed with smartphones have data and volume limits as part of their official duties, and if so, what are those limits and what happens if they are exceeded?

9. How is data usage and volume monitored and managed for police officers and staff with smartphones and other devices, and what measures are in place to ensure the security and privacy of the data stored and transmitted on these devices?

10. What specific brand and model of smartphones, Android devices, and Apple devices are issued to police officers and staff in Greater Manchester Police, and what is the total number of devices issued for each brand and model?

11. How often are smartphones and other devices issued to police officers and staff, and what is the process for replacing or upgrading devices that are lost, damaged, or outdated?

12. What type of training, if any, is provided to police officers and staff regarding the use of smartphones and other devices as part of their official duties, and how is the effectiveness of this training assessed?

13. How is the security of police-issued smartphones and other devices maintained, including measures to prevent unauthorized access or loss of data?

14. What is the preferred Browser support for Applications – i.e Microsoft Edge, Google Chrome, Firefox?

15. How does Greater Manchester Police ensure that the use of smartphones and other devices by police officers and staff aligns with relevant laws and regulations, including those related to data protection and privacy?

16. How does Greater Manchester Police assess the effectiveness and usefulness of the smartphone applications used by police officers and staff, and what feedback mechanisms are in place to gather input from users?

Result of Searches

Following receipt of your request searches were conducted within Greater Manchester Police (GMP) to locate the requested information and I can confirm the information requested is held by GMP.

However, I am not obliged to provide the information for questions 1 and 13 as an exemption applies.

Section 17 of the Freedom of Information Act 2000 requires Greater Manchester Police, when refusing to provide such information (because the 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.

Information relating to this request is exempted under **Section 31(1)(a)(b) – Law Enforcement**.

Section 31(1)(a)(b) is a prejudice based and qualified exemption, there is a requirement to articulate the harm that would be caused in disclosing any information held as well as carrying out a public interest test.

Harm

Disclosure of the number of officers allocated to specific units would reveal tactical capabilities and would compromise the efficient and effective conduct of the force. To disclose operational strength would hinder GMP in future law enforcement when policing Greater Manchester.

Additionally, disclosing and releasing information about mobile device security measures into the public domain could reveal weaknesses in GMP's IT systems. It could allow those with criminal intent to commit acts which would render GMP's systems vulnerable to cyberattacks.

Safety of the public is of paramount importance to the policing purpose, and release of this type of data could compromise any personal information GMP may hold. As such, GMP will not jeopardise the organisation's ability to do this through disclosing potential weaknesses into the public domain.

Furthermore, disclosing the number of officers allocated to neighbourhood policing would compromise the safety of the public that GMP serve to protect. There would also be a greater impact on police resources in that this could hinder the prevention and detection of crime, and more crime being committed.

At present the UK faces a sustained threat from violent terrorists and extremists, and it is particularly important for this reason to also withhold data of this nature in order to prevent such individuals from mapping police capabilities, potentially identifying 'weak points'.

Factors in favour of disclosure

The factors considered in favouring the disclosure of policing levels information are as follows:

To disclose how many officers are allocated to neighbourhood policing would show accountability of GMP in performing a key policing function. Disclosure would encourage public awareness and debate and may reduce crime or lead to more information being provided to GMP from the public for the prevention and detection of crime. Disclosure could be seen how GMP are using its resources to prevent crime.

Disclosure of mobile device security functions would make GMP more transparent and open to the general public allowing a brief insight to how GMPs mobile devices work. Furthermore, there is always a need to disclose information which relates to the spending of public money. It is in the public's interest to see how public funds are spent and it would be reassuring to the public to know that confidential data is safeguarded and how operational resources are balanced across the force area.

Factors against disclosure

To disclose how many officers are allocated to neighbourhood policing would compromise the efficient and effective conduct of the force, especially the force's future law enforcement tactics being compromised. The safety of the public is of paramount importance to GMP and to

release the requested information would compromise the safety of the community that GMP serve to protect and place individuals at risk.

The release of information relating to mobile device security could lead to cyberattacks on the force systems by those with the intent on committing such acts. Additionally, is also the risk to the public and their personal data, therefore seriously compromising the very safety of the public that GMP serves to protect.

Disclosure would lead to a greater impact on police resources, in that this could hinder the prevention and detection of crime and more crime being committed. It would give advantage to those individuals intent on criminal activity as it may assist potential criminals in evading the police as more vulnerable areas of lower policing levels would become evident. A fear of crime will be realised as gangs identify vulnerable areas and target and exploit these areas resulting in the public being in fear of more criminal activity occurring.

At present the UK faces a sustained threat from violent terrorists and extremists, the threat of terrorism and organised crime could increase as more crimes may be committed as a result of individuals gaining knowledge about the force's capabilities and therefore the public will be placed at a greater risk.

Balancing Test

When balancing the public interest Greater Manchester Police has to 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 GMP's accountability. This needs to be weighed against the strongest reason for non-disclosure which is the police service is charged with enforcing the law; preventing and detecting crime and protecting the people/communities we serve.

In this case, due to the fact that individuals may be placed at risk of harm and the affect it may have on the prevention and detection of crime I believe the case for disclosure is not made out.

The safety of the public is of paramount importance. The police will not divulge any information that would place the safety of an individual at risk or undermine law enforcement. Whilst there is a public interest in the transparency of policing, and in this case providing assurance that the police service is appropriately and effectively engaging with the threat posed by criminal activity and taking proactive measures to prevent unauthorised access to policing information, there is a very strong public interest in safeguarding operational capacity and security measures.

In accordance with the Act, this letter represents a Refusal Notice for questions 1 and 13 of your request.

2. Approximately 9,000.
3. Every Operational Police Officer is provided with a smartphone as are most Police Staff. Certain staff members whose role is desk based and requires a fixed landline phone are not issued a Smartphone. Only Android Smartphones are issued currently. GMP does not currently issue tablets.

4. Approximately 9,000.
5. 0.
6. On top of the standard accessibility functionality of the device, such as contrasting colours and fonts, apps comply with WCAG 2.1. Additionally Speak-to-text functionality is in-built in most apps.
7. GMP has a full Access to Work assessment system in place. Any requests for reasonable adjustments to allow officers and staff to work effectively are assessed by a qualified assessor, their recommendations considered and, if reasonable, are implemented. There are a number of Access to Work applications currently in use for GMP staff and all requests are reviewed on a case-by-case basis and if further software that is not currently supported is required, this is explored and provided where reasonable.
8. All GMP SIMs come with unlimited calls and texts barring premium rate numbers. All data comes via an organisational wide data allowance, in the region of 54TB per month. This has not been exceeded to date. Excessive usage falls under the appropriate use of information and technology procedure.
9. Like many other organisations GMP makes use of a Virtual Private Network (VPN) for its mobile devices, and the physical devices are subject to encryption through a mobile device management (MDM) system to ensure the security of stored and transmitted data. The data usage is monitored through a business relationship with the network.
10. The models currently in use by GMP staff are
 - Samsung Galaxy S9 (SM-G960F)
 - Samsung Galaxy S10 (SM-G973F)
 - Samsung Galaxy A40 (SM-A40FN)
 - Samsung Galaxy A52 (SM-A528B)

There are approximately 9,000 devices in use, but the exact number of these change regularly with breaks, repairs, losses and damages so the exact number is not easily retrievable and quickly out of date.

11. Staff are issued a smartphone when they begin employment with GMP, subject to their availability. GMP work with SSS public safety to provide a replacement and break/fix service. Phones are upgraded periodically as part of a technology refresh when the need arises and the budget is authorised.
12. The training delivered is about the policing application, and how data can be accessed off the system, the learners are given a number of independent tasks to complete and retrieve results. Learners are given a policy document for the usage of the devices.

The learners are summarily assessed and those identified to be struggling, their line managers are notified so additional support can be offered on districts.

No specific training is given for non-police specific applications, such as email and messaging apps but web training is available on the Force Intranet site.

14. Microsoft Edge.

15. All Police Officers and staff undertake significant data protection and legal training relevant to their role both on entering the organisation and as continuous professional development throughout their employment. Access to any policing data is regulated, monitored and audited at all times and all GMP Officers and staff are aware of this. Any breaches are dealt with robustly.
16. GMP maintains a large network of superusers across the force who constantly provide feedback and assessment of the applications deployed to them to the relevant team. All staff can contact a superuser or the team directly via email at any time.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]