| Police Scotland logo | Freedom of Information ResponseOur reference: FOI 23-0952Responded to: 04 May 2023 |
| --- | --- |

Your recent request for information is replicated below, together with our response.

## How many police officers are currently assigned to Local Policing Teams and Community Policing Teams in Police Scotland as of 8th April 2023?

As of 25 April 2023 there are 5,330 officers in Local Policing Teams and 2,263 officers in Community Policing.

## How many police officers and staff in Police Scotland are currently issued with a Smartphone as part of their official duties as of 8th April 2023

13,192 officers and staff are issued with smartphones.

## 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?

In response to this question, please see the table below.

| DEPARTMENT | DEVICE |
| --- | --- |
| Response Policing | Smart Phone |
| Community Policing | Smart Phone |
| CID | Smart Phone and tablet |
| Major Investigation Teams | Smart Phone and tablet  |
| Specialist Crime Division  | Smart Phone |
| Operational Support Division | Smart Phone |
| Special Constables | Smart Phone  |
| Forensics | Smart Phone |
| Probationer Training | Smart Phone |
| Partnership, Prevention and Community Wellbeing | Smart Phone |
| Traffic | Smart Phone |
| Armed Response | Smart Phone |
| Road Policing / Trunk Road Policing | Smart Phone |

## How many police officers and staff in Police Scotland are issued with Android Devices or tablets as part of their official duties as of 8th April 2023?

The number of officers and staff issued with phones is 13,192. The number of officers who have also been issued with tablets is 2,070. This is a total of 15,262 devices

## How many police officers and staff in Police Scotland are issued with Apple Device or tablets as part of their official duties as of 8th April 2023?

As of the 8th April 2023 no Apple devices or tablets are issued to Police Scotland Officers or Members of Police Staff.

## 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?

The Police Scotland system complies with WCAG 2.1 AA standards which are now a legal requirement for all web and mobile software used by public sector organisations. This ensures the application works with a range of assistive technologies and should also mean operation is clear and simple for all users.

Third party apps come as supplied and will follow whatever guidelines the developer includes within the app; Police Scotland have no control over these. As all our phones are Android devices, they have all the accessibility options Google provide with that O/S and device.

## 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?

As earlier noted, the system complies with WCAG 2.1 AA standards and this allows users to adjust settings if required to suit personal preferences/requirements.

## 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?

By default, data and volume limits are not imposed on officers or staff as part of their duties.

## 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?

Data usage and volume are not directly monitored, beyond reviewing the billing information from the network providers. In the event that a user is using an excessive amount of data, we reserve the ability to put restrictions in place to set individual data limitations on that device.

All the devices use multi-layer containerised encryption. All of the Apps on the device which are used for policing purposes use encrypted communication.

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

In response to the question above, in terms of Section 16 of the Freedom of Information (Scotland) Act 2002, I am refusing to provide you with the information sought. Section 16 requires Police Scotland when refusing to provide such information because it is exempt, to provide you with a notice which:

(a) states that it holds the information,

(b) states that it is claiming an exemption,

(c) specifies the exemption in question and

(d) states, if that would not be otherwise apparent, why the exemption applies.

The exemptions that I consider to be applicable to the information requested by you are:

Section 31(1) – National Security and Defence

Section 35(1)(a)&(b) – Law Enforcement

Section 39(1) – Health, safety and the environment

## Section 31(1) – National Security and Defence

Information is exempt information if it is required for purpose of safeguarding national security.

Disclosure of this information could undermine any ongoing or future operations to protect the security or infrastructure of the United Kingdom and increase the risk of harm to the public.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

This is a non-absolute exemption and requires the application of the Public Interest Test.

## Section 35(1)(a)&(b) – Law Enforcement

If the information was disclosed it could assist groups, organisations and those with hostile intent to identify, with some accuracy, Police Scotland’s technological capabilities and take steps to attack or hijack known vulnerabilities to Police systems directly or the supply chain. To provide the requested data could assist those with intent on doing harm with a tactical advantage when planning or perpetrating criminal plans and unlawful activities and maximise the impact of destruction, harm and disruption that may be caused.

Disclosure could have a negative effect on national security should the release of information be used and manipulated by criminal fraternities to try and attack politicians, public figures and other protected establishments and individuals.

Information is exempt information if its disclosure under this Act would, or would be likely to prejudice substantially the prevention or detection of crime and the apprehension or prosecution of offenders.

This is a non-absolute exemption and requires the application of the Public Interest Test.

## Section 39(1) – Health, safety and the environment

The disclosure of the information requested may have the potential to increase the number of attacks on public figures, operational police officers and members of the public and the potential to present a risk to an individual’s personal safety.

## Public Interest Test

I would suggest that public accountability may favour disclosure, given that the information concerns the efficient and effective use of resources by the Service. Likewise, disclosure of the information would also inform the public debate on the issue of policing and contribute to the accuracy of that debate.

However, any disclosure under FOI legislation is a disclosure to the world at large and any information identifying the focus of policing activity could be used to the advantage of criminals.

Consequently, in terms of the applicability of the exemptions listed above, the need to ensure the effective conduct of the service in relation to prevention and detection of crime and the public safety considerations involved in the delivery of operational policing clearly favour non-disclosure of the information requested.

It is important to note that the UK faces a serious and sustained threat from violent extremists and this threat is greater in scale and ambition than any terrorist threats in the past. The police service has a duty to promote the safety of all individuals, whether protected or not, and will not reveal any information that might jeopardise this goal. To provide details of resources allocated to their protection is likely to place individuals at serious and increased risk.

Accordingly, I would argue that the need to ensure the efficient and effective conduct of the service favours non-disclosure of the information requested and on balance is significantly in the public interest. I cannot identify any corresponding viewpoint in disclosing the requested information and therefore the exemptions are upheld.

I must advise you that it is doubtful it could ever be in the public interest to disclose information which would jeopardise the delivery of policing and the safety of individuals and prejudice the prevention or detection of crime.

To be of assistance I can advise that the security policies on the devices are determined in consultation with our Cybersecurity and Information Management teams and considered on the basis of manufacturer’s recommendations and industry best practice.

## 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?

If a device is damaged the user must report to the ICT Service Desk and thereafter inform their line manager. The device is then returned to ICT via the local Business Admin Unit. The user would then revert to using a paper notebook until a replacement device has been issued.

Mobile devices are refreshed periodically to ensure staff have access to the most up to date technology.

## 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?

Police Scotland provides formal training to operational officers and staff who require to use a Police Scotland Mobile Device to access and update Police Applications in the course of their duties.

The training is two-fold, and requires students to complete an e-learning pre-requisite before coming on a one day face-to-face course. The purpose of the training is to cover the functionality associated with the Mobile Device.

 The e-learning element covers the functionality aspects of searching via the device, such as Person/Vehicle searches across a variety of Police Applications that the Mobile Device can access, to ensure knowledge of how to search and how to interpret results. The e-learning module is assessed, with a pass/fail.

The one day face to face course enables hands on training covering the device and associated applications. This course further builds upon the content covered within the e-learning module and is also assessed.

The effectiveness of the training is assessed through the use of a training evaluation process, as well as engagement with key stakeholders and the Mobile Working development team to ensure training remains accurate, relevant and fit for purpose.

No formal training is provided to officers/staff who use a smartphone as a corporate device for example using e-mail/intranet/phone only.

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

In response to this question please see the response to question 10.

To be of assistance I can advise that the security policies on the devices are determined in consultation with our Cybersecurity and Information Management teams and considered on the basis of manufacturer’s recommendations and industry best practice.

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

The only browser on the devices is the Blackberry Access Browser. We do not allow Microsoft Edge, Google Chrome, Firefox on the devices.

## How does Police Scotland 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?

On passing the relevant training courses officers are required to sign a declaration on a ‘Conditions of Use’ form. This form clearly sets out prohibited activities and an Officer/ Police Staff responsibilities in respect of use of devices, relevant data protection regulations and privacy.

In addition to this users must complete a Data Protection learning module followed by a yearly refresher.

## How does Police Scotland 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?

We have a dedicated team to look after the Mobile estate, as well as IT Service Delivery teams who work with our users to ensure their needs are being met and will take feedback from users. Additionally, users have the ability to provide direct feedback on incidents and requests.

Engagement sessions are also undertaken across the country which provide valuable frontline feedback from users.

If you require any further assistance please contact us quoting the reference above.

You can request a review of this response within the next 40 working days by email or by letter (Information Management - FOI, Police Scotland, Clyde Gateway, 2 French Street, Dalmarnock, G40 4EH). Requests must include the reason for your dissatisfaction.

If you remain dissatisfied following our review response, you can appeal to the Office of the Scottish Information Commissioner (OSIC) within 6 months - [online](http://www.itspublicknowledge.info/Appeal), by email or by letter (OSIC, Kinburn Castle, Doubledykes Road, St Andrews, KY16 9DS).

Following an OSIC appeal, you can appeal to the Court of Session on a point of law only.

This response will be added to our [Disclosure Log](http://www.scotland.police.uk/access-to-information/freedom-of-information/disclosure-log) in seven days' time.

Every effort has been taken to ensure our response is as accessible as possible. If you require this response to be provided in an alternative format, please let us know.