| Police Scotland logo | Freedom of Information Response Our reference: FOI 23-1385  Responded to: 16th June 2023 |
| --- | --- |

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

**I am writing under the Freedom of Information Act 2000, to make a request for information relating to your organisation’s development and/or use of digital decision tools for policing and law enforcement.**

**By digital decision tools, I mean any technology that uses software algorithms to process digital data and generate outputs either to (a) \*support\* policing decisions, by providing information or recommendations to a human police officer, who retains discretion in making the final decision; or (b) \*automatically\* trigger a policing or law enforcement decision based on the generated output(s).**

**By ‘policing and law enforcement decisions’, I mean any decisions taken by police officers in carrying out their duties to detect and prevent crime, to protect the public and reduce harm, to maintain public order, to enforce the law, and to bring offenders to justice. This may include (but is not limited to) decisions concerning the imposition of enforcement notices (e.g., speeding fines), case/complaints-handling, resource allocation, criminal investigations (particularly those concerning whether to pursue inquiries in relation to specific persons, and what action(s) to take, such as arrest or questioning, stop and search etc.), and decisions made at the pre-trial stage about individuals, including detention and charging decisions.**

**EXAMPLE TOOLS OF INTEREST**

**To help with my inquiry, examples of the kinds of tools I am requesting information on tools including:**

**1. \*Digital dashboards\*: any tool which processes and organises data sets to generate data visualisations to assist policing work. For example, they might provide information about ongoing and/or recently reported incidents, the analysis of crime patterns, workload and resource allocation, and data shared with public agencies such as the emergency services. These dashboards might, for instance, be used to improve emergency response times, assist officer decision-making, resource management, and so on. For example, Qliksense.**

**2. \*Individual risk assessment tools\*: any tool which processes data to generate predictions about the ‘risk’ posed by an individual relating to an undesirable outcome, such as their risk of committing a serious violent crime in the future, risk of general recidivism, risk of self-harm, or risk of becoming a victim of harm. For example, the London Gangs Matrix or the Harm Assessment Risk Tool (‘HART’) that has previously been used by Durham Constabulary.**

**3. \*Geospatial crime ‘hotspot’ mapping tools\*: any tool which processes historical crime data to identify patterns indicating potential crime ‘hotspot’ areas (i.e., geographical locations where crime is predicted to be most likely to occur within a given time period). For example, PredPol.**

**4. \*Automated biometric analysis tools\* (including live facial recognition systems): any tool which processes biometric data for the purposes of identifying individuals ‘of interest’ (i.e., according to s.205 of the Data Protection Act 2018: biometric data is data relating to the physical, physiological, or behavioural characteristics of a person, such as facial images, fingerprints, or retina scanning). For example, NeoFace Watch.**

**5. \*Any other tool to assist policing and law enforcement work\*: any other tool that uses software algorithms to generate outputs to help inform policing decisions made by your organisation, or to automatically trigger decisions based on those outputs (e.g., Automated Number Plate Recognition (ANPR) systems, social network analysis, case ‘solvability’ analysis, and so on).**

**--------------------------------------------------------------------------------------------**

**SPECIFIC INFORMATION REQUESTED**

**My specific information requests are listed and numbered below. Please provide information related to tools by your police force.**

**To help reduce the resources needed to respond to my numbered requests, you may limit your responses to \*ten\* tools.**

**If your organisation has deployed \*ten or fewer\* tools in total (including those currently deployed, in development, being piloted or formerly developed or piloted but never deployed), please skip straight to the numbered requests below.**

**If your organisation has deployed and/or is developing (or has developed) \*more\* than ten tools in total, please respond to the numbered requests for the ten \*most recently\* deployed.**

**FOR EACH RELEVANT TOOL (UP TO TEN IN TOTAL), CAN YOU PLEASE:**

**1. Supply the \*name(s)\* of each tool.**

**2. Explain the \*reason(s)\* why your organisation decided to develop and/or deploy each tool, including the intended \*policy purpose(s)\* of the tool (e.g., to reduce criminal offending by aiming to improve the identification of potential victims of a criminal offence or to identify individuals ‘of interest’ to police, using the automated analysis of digital data).**

**4. Identify the data sources used as ‘inputs’ to the tool and indicate whether this data has been collected from internal police data sources (e.g., crime data), external public-sector data sources (e.g., data held by local authorities), or external data sources made available by private-sector organisations (e.g., mobile communications data). Please further indicate whether the tool is updated with new data on a manual basis, by a human user responsible for inputting data (including how frequently this usually occurs), or if it is updated on a real-time basis using an automated live data feed.**

**5. Identify the \*output(s)\* that each tool produces/produced in order to serve its intended policy purpose, and what these outputs are taken to \*indicate or signify.\* For example: an individual risk assessment tool may produce a ‘risk classification’ for each assessed person (e.g., ‘high’, ‘medium’ or ‘low risk’). What is it, specifically, that each person is at ‘high risk’ or ‘low risk’ of, in this scenario (e.g., being arrested under suspicion of having committed a serious offence within the next two years)?**

**6. Indicate the kind(s) of \*decision(s)\* each tool supports/supported or triggers/triggered and about \*whom or what\*? For example: who to stop and search? Where to send police patrols? Should an arrested person be retained in police custody?**

**7. Identify the \*intended user(s)\* of each tool. For example: does/did the tool provide information to a front-line officer on patrol, a duty officer in a custody suite, both, or someone else?**

**8. Please indicate whether in relation to each tool, users receive any \*training\* about tool-use, indicating what that training consists (or consisted) of, who provides this training (including whether this is in-house or external), and who receives training.**

**9. Indicate the \*date(s)\* when each tool was first deployed (and when its use was ended, if applicable).**

In response to all of the questions within your request, I regret to inform you that I am unable to provide you with the information you have requested, as it would prove too costly to do so within the context of the fee regulations.

As you may be aware the current cost threshold is £600 and I estimate that it would cost well in excess of this amount to process your request.

As such, and in terms of Section 16(4) of the Freedom of Information (Scotland) Act 2002 where Section 12(1) of the Act (Excessive Cost of Compliance) has been applied, this represents a refusal notice for the information sought.

By way of explanation, your request is fairly broad in scope and Police Scotland do not hold a central repository of information which catalogues the information required to answer your request. Police Scotland have over 800 systems as well as hundreds of Business Intelligence/Management Information dashboards. These would all need to be examined to determine if they met the criteria of your request and then the date implemented compared if there were more than 10.

Whilst I note you have asked for only the 10 most recent examples that meet your criteria to be included to reduce the scope of your request. The initial sift of systems to determine what should and should not be included would take a large amount of time to complete.

Police Scotland have assessed that the £600 cost limit within the Act equates to 40 hours of work and that your request would breach the cost threshold.

Whilst I would normally suggest a revised timescale is considered, in this case as the initial sift would be largely the same I do not believe this would assist. You may wish to consider reducing the scope of your request to a less broad definition.

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](mailto:foi@scotland.police.uk) 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](mailto:enquiries@itspublicknowledge.info) 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.