

9 December 2025

FOI Ref 22051

Request - You asked us the following:

1. Data-sharing agreements / MoUs – copies of any memoranda of understanding, data-sharing agreements, written protocols or other arrangements between Staffordshire Police and Moog Aircraft Group UK (or its private-security contractors) permitting the sharing of CCTV footage, still images or biometric/visual identifiers.

2. Requests / disclosures of imagery – records or logs showing the number and dates of requests by Staffordshire Police to Moog (or its contractors) for CCTV or still-image material, and the number and dates of disclosures by Staffordshire Police of such imagery to Moog (or its contractors). If individual records cannot be released, please provide an anonymised summary table (date, parties, short subject).

3. Facial-matching / AFR / LFR – any documents, policies, or records describing or authorising use of Automated Facial Recognition (AFR), Live Facial Recognition (LFR) or manual facial-matching processes in relation to protests or incidents near Moog sites, including any Data Protection Impact Assessments.

4. Third-party imagery sharing – any correspondence or agreements describing the sharing of imagery, facial templates or watchlist information between Staffordshire Police and – Moog Aircraft Group UK; – Moog's private-security contractors; or – the Home Office, NPCC or other forces for the purpose of identifying protest participants.

I am not requesting evidential material from ongoing prosecutions; I recognise such material may be exempt under sections 30–31 FOIA. Where information is withheld, please specify the exemption(s) relied upon, indicate the extent of withheld material, and supply redacted versions or summaries where feasible.

If complying in full would exceed the cost limit, please prioritise items 2 and 4 and advise how to narrow the remainder under section 16 FOIA.

Staffordshire Police (SP) received your request on 04/11/2025 and have processed this under the Freedom of Information Act (FOIA).

Staffordshire Police's response to your enquiry is as follows:

SP holds/does not hold the requested information.

1. Data-sharing agreements / MoUs – copies of any memoranda of understanding, data-sharing agreements, written protocols or other arrangements between Staffordshire Police and Moog Aircraft Group UK (or its private-security contractors) permitting the sharing of CCTV footage, still images or biometric/visual identifiers. – **Neither confirm nor deny.**

2. Requests / disclosures of imagery – records or logs showing the number and dates of requests by Staffordshire Police to Moog (or its contractors) for CCTV or still-image material, and the number and dates of disclosures by Staffordshire Police of such imagery to Moog (or its contractors). If individual

records cannot be released, please provide an anonymised summary table (date, parties, short subject).
– **Neither confirm nor deny.**

3. Facial-matching / AFR / LFR – any documents, policies, or records describing or authorising use of Automated Facial Recognition (AFR), Live Facial Recognition (LFR) or manual facial-matching processes in relation to protests or incidents near Moog sites, including any Data Protection Impact Assessments. – **Neither confirm nor deny.**

4. Third-party imagery sharing – any correspondence or agreements describing the sharing of imagery, facial templates or watchlist information between Staffordshire Police and – Moog Aircraft Group UK; – Moog's private-security contractors; or – the Home Office, NPCC or other forces for the purpose of identifying protest participants. – **Neither confirm nor deny.**

The following exemption has been applied:

In accordance with Section 17(1) of the Freedom of Information Act, this letter represents a refusal notice for this particular request.

- Section 31(3) - Law Enforcement.

The duty to confirm or deny does not arise if, or to the extent that, compliance with Section 1 (1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

- Section 24 (1) – National Security

Section 24 is a qualified exemption and as such there is a requirement to articulate the harm and conduct a test of the public interest.

Harm:

Confirmation or denial that any further information is held relevant to this request would be likely to prejudice both law enforcement and national security. Revealing details of data-sharing agreements, imagery requests, or facial recognition processes could assist individuals or groups in understanding operational policing tactics and surveillance capabilities. This knowledge could be exploited to evade detection, disrupt investigations, or compromise the security of critical infrastructure. Such disclosure would undermine the ability of SP to prevent and detect and could create vulnerabilities that threaten national security. Any disclosure that undermines the generic terms of duty of care provided by policing and Law Enforcement would be detrimental to the public at large. In short, any incident that results from confirming that any other information is or isn't held would by default affect National Security.

Public Interest Test

Factors favouring confirming or denying information is held under Section 31

To confirm or deny that information is held would adhere to the basic principle of being open and transparent, it would also lead to a better public awareness of the workings of the police force and the communications used with intelligence, operations and during routine policing.

Factors against confirming or denying information is held under Section 31

Confirming or denying whether the requested information is held could prejudice the prevention or detection of crime and undermine law enforcement capabilities. Disclosure of even the existence of such

information may reveal operational tactics, surveillance methods, or collaborative arrangements, which could be exploited by individuals seeking to evade detection or disrupt policing activities. It could also compromise ongoing investigations or future operations by providing adversaries with insight into law enforcement strategies. Maintaining the ability to neither confirm nor deny is therefore essential to protect the integrity of policing and ensure public safety.

Factors favouring confirming or denying information is held under Section 24

To confirm whether any other information is held relating to this request would better inform the general public as to the existence of policing and law enforcement capabilities within specific geographical locations. In turn, this can increase public confidence with the likely effect of dissuading mal-actors from operating within specific areas or regions.

Factors against confirming or denying information is held under Section 24

Confirming or denying whether the requested information is held could compromise national security by revealing the existence or absence of sensitive security measures. Even acknowledging that such information exists may provide adversaries with insight into protective strategies, surveillance capabilities, or vulnerabilities, which could be exploited to target critical infrastructure or plan hostile acts. Maintaining the ability to neither confirm nor deny is essential to safeguard national security interests, protect operational integrity, and prevent risks to public safety.

Balance test

When considering whether disclosure is appropriate, SP must weigh the strongest reason for disclosure against the strongest reasons for non-disclosure. In this case, whilst the factors favouring disclosure are important in that it would adhere to the basic principle of being open and transparent, SP believe when weighed against the risk of disclosure undermining our ability to prevent and detect crime and hindering our ability to protect the public, then non-disclosure takes precedence.

Please be advised that all Freedom of Information request responses are published on the SP website although personal details are not included.

Freedom of Information Request Appeals Procedure

1. Who Can Ask for a Review

Any person who has requested information from SP, which has been dealt with under the Freedom of Information Act, is entitled to complain and request an internal review, if they are dissatisfied with the response they received.

2. How to Request a Review

Requests for review of a Freedom of Information request must be made in writing within two months of the date of receipt of this email, and should be addressed to:

IAT@staffordshire.police.uk

Or by Post to:

Information Access Team
Staffordshire Police HQ



STAFFORDSHIRE
POLICE

PO Box 3167
Stafford
ST16 9JZ

The reference number, date of the request and details of why the review is being requested must be included. Requests for review should be brought to the attention of the Information Access Team within two months of the Force's response to the original FOI request.

3. Review Procedure

Receipt of a request for review will be acknowledged in writing. The review will be conducted by a Supervisor who is independent from the original Decision Maker. The Information Access Team will set a target date for a response. The response will be made as soon as is practicable with the intention to complete the review within 20 working days. In more complex cases the review may take up to 40 working days.

The independent Supervisor will conduct a review of the handling of the request for information and of decisions taken, including decisions taken about where the public interest lies in respect of exempt information where applicable. The review enables a re-evaluation of the case, taking into account the matters raised by the complaint.

4. Conclusion of the Appeal

On completion of the review the Independent Supervisor will reply to the appellant with the result of the review. If the appellant is still dissatisfied following the review they should contact the Information Commissioner to make an appeal. The Information Commissioner can be contacted via the following link:
<https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Freedom of Information
Information Access Team