

Gloucestershire Constabulary
Police Headquarters
No.1 Waterwells, Waterwells Drive
Quedgeley, Gloucester. GL2 2AN
www.gloucestershire.police.uk



Our reference: FOI_26_0793

E-mail: FOI@gloucestershire.police.uk

Direct dial: 01452 754304

Postal Address: As above

Date: 05/10/2026

Dear

Gloucestershire Constabulary Freedom of Information request FOI_26_0793

On 24/08/2026 you sent an email constituting a request under the Freedom of Information Act asking the following:

Please provide the following information for the period 1 July 2024 to the date on which this request is processed. If your force has not used a particular form of facial recognition during that period, please state this clearly and continue to answer any remaining sections that are applicable.

1. Compliance with deletion and retention requirements

For each live facial recognition (LFR) deployment during the above period, please provide the deployment date and location together with any recorded confirmation, certification, checklist entry, audit entry or equivalent record confirming that the required post-deployment deletion of LFR data was completed.

I am not seeking the personal data itself. I am seeking the recorded evidence demonstrating that deletion took place.

Please also provide the number of occasions during this period on which any of the following were retained beyond the ordinary retention period specified by force policy or applicable governance documentation:

a. biometric templates relating to individuals who did not generate an alert; b. probe images or biometric templates associated with an alert; c. candidate/watchlist images or associated biometric templates uploaded to an LFR system; d. data remaining on media used to import a watchlist; and e. CCTV footage created as part of an LFR deployment.

Where the number for any category is greater than zero, please provide, in aggregate form, the deployment concerned, type of information involved, length of the retention

overrun, the recorded reason for the overrun and whether it resulted in a data-protection or information-security incident being recorded.

This request does not require disclosure of the identity of any data subject.

2. Audit and assurance

Please provide copies of any final internal audit, compliance review, assurance review or equivalent report produced since 1 July 2024 which examined compliance with facial-recognition data-retention or deletion requirements.

Where a wider report concerns several subjects, I am content to receive only those pages or sections dealing with facial-recognition retention, deletion, disposal or audit.

Please additionally provide:

a. the dates of any periodic audits of facial-recognition deletion/retention; b. the recorded outcome or conclusion of each such audit; c. details of any recommendations or corrective actions arising from those audits; and d. whether each recommendation has been recorded as completed, outstanding or otherwise closed.

Where the facial-recognition application used by the force has audit-trail functionality, please confirm what types of deletion-related audit event the system records, whether automatic deletion of non-matching biometric templates generates or can be evidenced by an audit record, and the retention period applying to those audit records.

I am seeking the categories of audit information and retention arrangements, not security-sensitive configuration information or individual user credentials.

3. Verification that deleted data cannot subsequently be recovered

Please provide any recorded test, technical assurance, acceptance test, audit report or supplier assurance held by the force which verifies that deleted facial-recognition probe images and biometric templates are non-retrievable.

For each such assurance exercise, please provide the date, whether it was conducted internally or by an external organisation, and its recorded conclusion.

If no independent or technical verification of non-retrievability has been undertaken or is held, please state this explicitly.

Please also state whether facial-recognition probe images or biometric templates may, before deletion, be copied or replicated into any temporary file, cache, backup, removable storage, diagnostic record or other persistent storage outside the principal facial-recognition application. If so, please provide the retention/deletion rule applicable to that copy.

Again, I do not request network architecture or exploitable technical security information.

4. Data-protection and information-security incidents

Please provide the number of recorded incidents since 1 July 2024 involving:

a. failure or delay in deleting facial-recognition data; b. unauthorised retention of facial-recognition data; c. unauthorised access to facial-recognition data; or d. facial-recognition data remaining on equipment or storage media beyond its authorised retention period.

For each category, please state how many incidents were assessed as personal-data breaches and how many, if any, were reported to the Information Commissioner's Office.

Aggregate figures are sufficient and no personal information relating to affected individuals is requested.

5. Retrospective and Operator Initiated Facial Recognition

Please confirm whether the force has used either Retrospective Facial Recognition (RFR) or Operator Initiated Facial Recognition (OIFR) at any time since 1 July 2024.

For each technology that has been used, please provide the current:

- a. policy or operating procedure;
- b. Data Protection Impact Assessment;
- c. Appropriate Policy Document, where one exists; d. retention/deletion schedule applicable to probe images, biometric templates and candidate results; and e. any audit or assurance document addressing compliance with those deletion requirements.

Please also identify, at a high level, the reference database or databases against which such searches are conducted. I do not seek information about any individual search or investigation.

6. Appropriate Policy Documents, suppliers and third-party processing

Please provide the current Appropriate Policy Document or equivalent governance document applying to the force's use of LFR, RFR and/or OIFR, where held and not already provided above.

Please also identify the supplier(s) of the facial-recognition systems used by the force for LFR, RFR and OIFR and state, for data-protection purposes, whether each organisation acts as a processor, sub-processor, separate controller, joint controller, or has no access to police biometric data.

Where the force holds a contract schedule, data-processing agreement or information-sharing agreement governing supplier access to, retention of or deletion of facial-recognition data, please provide the portions dealing with those subjects.

Under the Freedom of Information Act 2000 s1, I can confirm that Gloucestershire Constabulary holds no relevant information.

In relation to your request, searches were conducted by the relevant business areas and no information is held.

If you are not satisfied with this response or any actions taken in dealing with your request, you have the right to ask that we review your case under our internal procedure. Please note that a request for an internal review must be made within 20 working days of the response to your original request.

If you decide to request that such a review is undertaken and following this process you are still unsatisfied, you then have the right to direct your complaint to the Information Commissioner for consideration.

The Information Commissioner can be contacted via the following means:

Website - <https://ico.org.uk/>

Call their helpline - 0303 123 1113

Email - casework@ico.org.uk

Post – Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Yours sincerely,

Disclosure Officer
Gloucestershire Constabulary