Home Office

Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies

Government response

Published on: 4 November 2026

Contents

Introduction and contact details 2
Complaints or comments 2
1. Introduction 3
2. Summary of responses 5
3. Impact Assessment, Equalities and Welsh Language 17
Impact Assessment and Equalities Impact Assessment 17
Welsh Language Impact Test 17
4. Consultation principles 18

Introduction and contact details

This document sets out the Government's response to the public consultation: Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies (accessible).

It covers the:

Introduction

Background to the consultation

Summary of the consultation responses

Next steps following this consultation.

Further copies of this report and the consultation paper can be obtained by contacting Data & Technology Policy & Strategy at the address below:

Data & Technology Policy & Strategy
Home Office
2 Marsham Street
London SW1P 4DF

Email: fr-consultation@homeoffice.gov.uk

This report is also available at https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement.

Alternative format versions of this publication can be requested by email to fr-consultation@homeoffice.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Home Office at the above address.

1. Introduction

The Government is grateful to everyone who responded to the consultation on developing a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies, which was published on 4 December 2025. The consultation process was extensive and played an important role in informing the Government's approach to designing a new legal framework.

The consultation sought views on key issues including which technologies should be covered, who the framework should apply to, when these technologies should be used, and what safeguards and oversight should be in place to protect privacy and other rights while enabling effective policing. The consultation closed on 12 February 2026.

This Government response summarises the views received and sets out the Government's high-level proposals for a new legal framework. In developing these proposals, we have:

- Undertaken engagement with a range of stakeholders including civil society groups, academics, law enforcement, commissioners and regulators.
- Considered findings from the previously published public attitudes research[1]. This research engaged a nationally representative sample of 3,920 adults in England and Wales and explored public awareness, as well as acceptability and associated concerns across different uses. Alongside consultation responses and targeted stakeholder engagement, this evidence provides important context, helping the Government to better understand areas of support, concern and differing views.
- Undertaken targeted engagement with under-represented groups [report of findings published here: Police use of facial recognition technology: a public dialogue - GOV.UK]

The consultation and engagement process has shown that there is public support for a specific legislative framework for law enforcement use of biometric technologies including facial recognition. However, we recognise there are differing views on how a future framework should be constituted.

The Government intends to introduce a new statutory framework for use of biometrics, facial recognition, and similar technologies by law enforcement and other public bodies. This framework will include specific powers and obligations for those authorised to use these technologies and it will ensure policing can innovate in a repeatable and consistent manner, supporting adoption of emerging biometric and overt surveillance technologies that improve policing effectiveness and public protection, while maintaining appropriate safeguards and oversight. The framework will also establish a new independent oversight

[1] https://www.gov.uk/government/publications/public-attitudes-to-police-use-of-facial-recognition-technology Public attitudes to police use of facial recognition technology - GOV.UK

body, which will consolidate and expand the functions of existing oversight roles and have powers to monitor compliance and enforce standards.

The new framework will also include measures to ensure consistency between law enforcement and private sector approaches, while recognising their distinct legal and operational contexts.

A Welsh language response paper will be made available alongside the English version – see the Welsh Language guidance at: https://www.gov.uk/government/organisations/home-office/about/welsh-language-scheme

2. Summary of responses

i. Consultation process and methodology

The consultation responses were received through an online questionnaire, which was available via a dedicated consultation portal. Responses were also received via email; in total we reviewed 12,584 emails. Of these, 588 were distinct email responses while 11,996* were identified as duplicate or non-consultation responses received in the inbox.

Duplicate text in emails was identified using similarity scores, with original messages isolated to extract the main ideas. Where content was identical, responses were analysed thematically once to avoid repetition. Each unique email was reviewed and coded to capture the breadth of concerns, positive views, possible personal impacts, recommendations, and expectations arising from the consultation. These emails remain part of the overall dataset.

We also analysed consultation responses received through an online form, with 1,261 completed responses out of 1,826 total entries. Responses that were only partially completed were excluded from both quantitative and qualitative analyses.

See Tables 1 and 2 for the volumes for each category and a detailed breakdown of how submissions were categorised.

Table 1. Volume of submissions

Metric	Description	Value
Total email submissions	588 unique submissions and 11,996 with either identical text or no consultation response	12,584
Completed online form responses	Completed entries	1,261
	TOTAL (fully submitted)	**13,845**

* this number includes a small number of administrative emails

Table 2. Broad categories of consultation respondents

Respondent category	Description
Members of the public	Individuals responding in a personal capacity, primarily via private email domains or the online consultation form.
Civil society and advocacy organisations	Organisations representing public interest, civil liberties, equality, and rights-based perspectives, including charities, NGOs, campaign groups and think tanks.
Academia and research organisations	Universities, academic institutions and research bodies.
Law enforcement bodies	Police forces, policing bodies and professional policing organisations.
Regulators and oversight bodies	Statutory regulators and oversight organisations with responsibilities relating to data protection, human rights, forensic science, accreditation or standards.
Public sector organisations	Government departments, local authorities and other public bodies responding outside a policing or regulatory role.
Industry and technology providers	Private sector organisations, including technology developers, suppliers and commercial users of biometric or surveillance technologies.

Respondent categories are indicative and reflect broad groupings based on available information. Responses were not analysed on a representative basis and respondents may fall into more than one category.

ii. Analytical approach

The consultation included both structured questions and open-ended text prompts. While most participants addressed the specific questions in the online form, some did not. As a result, responses were categorised according to pre-defined thematic policy areas while capturing the breadth of concerns voiced by respondents.

The principal themes from this analysis include:

- the scope of technologies
- who can use these technologies
- privacy and surveillance concerns
- proportionality, necessity and justification
- safeguards, oversight and governance

These themes are summarised in the sections that follow.

1. Privacy and surveillance concerns

To gather views on this objective of the new legal framework, two questions were asked on the online form:

- *What other factors are relevant to assessing interference with privacy?*
- *Which factors are relevant when assessing interference with other rights?*

Summary of consultation responses

i. Access to personal data

Respondents thought that the new framework should ensure personal data is handled appropriately after collection. This included mitigating potential risks around data security, breaches, unauthorised access, inappropriate sharing, and repurposing. Some also thought that consideration should be given to the risk of biometrics being combined with other datasets and the potential for increased privacy intrusion if data collected for different purposes were merged. Responses emphasised the need for strict limits on who can access data and for what purposes.

Data retention was also highlighted, with some noting that privacy intrusion increases the longer data is held. Some suggested the legislation should limit retention to defined periods and mandate the deletion of data when it is no longer necessary. Some respondents also expressed a lack of confidence in law enforcement bodies or technology suppliers' data handling practices.

ii. Consent

The ability to consent to or 'opt out' of facial recognition was also identified as a key theme. Some noted that meaningful choice would be difficult, particularly if large image databases were used. Transparency was a core expectation, with respondents supporting the police using the technology where there is a clearly defined purpose.

Some argued consent should be addressed at a local level and stressed that the public should always be informed when and where facial recognition technology is used. Advance notification was seen as important and many felt that it was important to ensure a genuine effort was made to ensure signage were adequately visible. Law enforcement respondents also emphasised the importance of transparency.

Concerns were raised about use of facial recognition technology in situations involving children and vulnerable adults who may not be able to give consent. A consistent view was that any legislation should specifically protect children from being subjects of facial recognition searches. Some advocacy groups warned that safeguarding purposes could have unintended consequences for individuals who do not wish to be located. They noted that this could potentially increase the risk of harm and argued that parents or legal guardians should be able to refuse inclusion on a watchlist in such cases.

iii. Civil liberties and public participation

Some respondents were also concerned about the potential for interference with peaceful assembly and freedom of expression. The "chilling effect" was mentioned, suggesting facial recognition technology could deter lawful activity and free use of public space. Those respondents raising civil liberties issues often said facial recognition should be prohibited at protests and demonstrations, fearing it could be used to target or discourage

participants. Advocacy groups warned this could disproportionately affect marginalised communities and further damage trust in law enforcement.

Respondents also described discomfort with constant observation, citing behavioural and psychological impacts such as anxiety and reduced willingness to move freely. Some argued this atmosphere would suppress free expression and participation in civic life.

iv. Trust in the relationship between the public and the state

Some respondents argued that facial recognition could undermine the presumption of innocence and lead the state to treat the general population as potential suspects. Fears were expressed about a drift towards a "surveillance state", eroding freedoms and expectations of privacy.

Others argued that innocent individuals should not be routinely included in watchlists, and that expanding biometric databases, such as through passport images, posed serious democratic risks by normalising monitoring, shifting power towards the state, and weakening public trust.

Some respondents questioned facial recognition technology's effectiveness, suggesting offenders would conceal their faces. Others feared police might be driven to enforce the removal of face coverings, seen as a further infringement of civil liberties and privacy.

v. Concerns about mass surveillance

Respondents raised concerns that facial recognition could be used beyond its original purpose and evolve into routine mass surveillance without binding limits. Some feared misuse by future governments, including for monitoring dissent, political opposition, or excluding individuals from public spaces.

A cohort argued that facial recognition should only be used where demonstrably necessary and where less intrusive options are unavailable. Some felt live facial recognition deployments should be temporary and for tightly defined purposes, rather than becoming a permanent fixture at a certain location. The overarching concern was about preventing tools authorised for specific operational purposes from becoming default mechanisms of state surveillance.

Government response

The Government agrees that technologies like facial recognition have the potential to interfere with rights, such as the right to privacy, freedom of expression and the right to peaceful assembly. Although there is already an established legal framework for use of facial recognition, the new framework will be designed to improve public confidence as use of these types of technology increases. That is why we intend to introduce new, specific laws governing their use. This new framework will build on the principles established in the Protection of Freedoms Act 2012 and will set out clear powers to acquire, retain and use biometrics alongside clear obligations on those who exercise those powers.

The framework will include detailed operational requirements and safeguards, building on existing police guidance but in a statutory Code of Practice. This will ensure law enforcement can properly harness the power of technologies like facial recognition into the future, but only where it is demonstrably justified, necessary and proportionate to do so. Through this new legal framework, the Government will balance the need to respect and preserve individual human rights with the rights of the public to be safe on the streets and in their communities.

2. Scope of the new legal framework

This section relates to consultation questions on the scope of a new legal framework governing police use of biometrics, facial recognition and similar technologies. The consultation asked for views on which types of technologies should be covered by the new framework, whether it should apply to all biometric technologies used by law enforcement, whether it should extend to inferential technologies, and whether it should include systems that identify clothing, belongings or objects. It also sought views on whether the framework should be flexible enough to accommodate emerging technologies over time.

The following questions were asked:

- *To what extent do you agree or disagree that a new legal framework should apply to all use of 'biometric technologies' by law enforcement organisations?*
- *Do you think a new legal framework should apply to 'inferential' technology i.e. technology that analyses the body and its movements to infer information about the person, such as their emotions or actions?*
  Should the framework apply to technology that can identify clothing, belongings or objects?
- *Should the framework be flexible enough to include new technologies?*

Summary of consultation responses

i. Types of biometric and similar data in scope of the framework

Among those that responded using the online form most agreed the framework should cover all biometric data types, including inferential technology and identification of clothing or objects. Respondents broadly agreed that biometric technologies, including facial recognition, are sufficiently sensitive to warrant a clear and specific legal framework. Many expressed the view that such technologies are inherently intrusive and should not rely on a patchwork of general powers or guidance alone. Across responses, consultees emphasised that clear statutory limits and safeguards were essential to maintaining public trust and preventing inappropriate expansion of use.

Some respondents raised concerns about inferential technologies, such as systems that attempt to infer a person's emotions or intentions and felt they should be in scope of a new framework. These concerns focused on the scientific validity of such tools, their reliability across different populations and contexts, and their compatibility with rights protections.

Some respondents argued that inferential technologies require either very strong restrictions within a new framework or wanted legislation to prohibit use altogether, while others favoured heightened scrutiny before it is permitted within the law.

Views on object, clothing and vehicle identification technologies were more mixed. Some respondents recognised that such tools could have limited investigative value in specific circumstances, particularly where facial images are unavailable. Others highlighted that these technologies could function as indirect identification or tracking tools, raising concerns about accuracy, proportionality and potential discriminatory impacts. Respondents therefore cautioned against treating such technologies as inherently low-risk within any future framework.

Respondents consistently raised the importance of ensuring that any framework remains effective in the face of rapid technological change, while avoiding overly permissive approaches that could enable unchecked expansion. Some favoured a technology-neutral or principles-based framework that could adapt to new tools without repeated legislative change. Others stressed the need for parliamentary scrutiny of new technologies, particularly where they present novel or heightened risks. Across these views, consultees highlighted concerns about mission creep, including the risk that technologies introduced for narrow purposes could gradually be used in more routine or expansive ways without sufficient public debate or safeguards.

ii. Who the new framework should apply to

Many respondents questioned whether limiting the framework to law enforcement organisations would create accountability gaps, particularly given private sector use of similar technologies and the existence of cross-sector partnerships. Concerns were raised about uneven regulation across sectors, the potential for surveillance capabilities to be outsourced, and the use of third-party datasets by police without consistent safeguards.

Other respondents argued that where biometric and facial recognition technologies are used to exercise coercive state powers, such as the power to arrest someone, law enforcement use raises distinct issues that justify a legal framework specific to law enforcement uses. Some respondents also expressed the view that private sector use should be tightly restricted or prohibited separately.

Government response

We agree confidence of both the police and the public would be improved by the introduction of a bespoke framework, with specific rules governing law enforcement acquisition, processing and retention of biometrics including facial images. We intend to introduce proposals for facial images which build on existing statutory rules for the collection, retention and use of biometric material, such as the legal framework governing DNA and fingerprints. We recognise technology capabilities are constantly evolving, so to remain resilient to future technological developments while ensuring appropriate accountability and scrutiny, the legislation will allow for a clear mechanism to extend the framework to other biometric data types in the future.

It is clear that the use of biometric technologies to make inferences about an individual's behaviour has the potential to impact on their privacy and other rights. Furthermore, we agree the use of overt surveillance tools to identify and track objects could impact privacy and other rights. In recognition of this, building on the principles established in the Protection of Freedoms Act 2012 and the current role of Surveillance Camera Commissioner, the new framework will also cover use of overt surveillance technologies and inferential technologies.

The Government will bring forward a framework that governs the use of biometrics, facial recognition and similar technologies by law enforcement organisations, including policing, and other public bodies, for law enforcement and limited safeguarding purposes. New powers will be supported by a statutory Code of Practice setting out the requirements for law enforcement organisations and other public bodies.

We acknowledge the appetite for greater consistency between law enforcement and private-sector use of technologies such as facial recognition. Private-sector use is already subject to existing data protection law, but we recognise the value of clearer and more practical guidance on how those requirements apply in practice. We are therefore committed to bringing forward a Code of Practice for private-sector use for the prevention and detection of crime, complementing the law enforcement framework while recognising the distinct legal and operational contexts in which these technologies are used.

3. Proportionality, necessity and justification

The consultation also sought views on legitimate purposes for use of facial recognition and similar technologies. To gather views on this proposal, the consultation asked the following questions:

- *Do you agree or disagree that 'seriousness' of harm should be a factor to decide how and when law enforcement organisations can acquire, retain, and use biometrics, facial recognition, and similar technology?*
- *What factors do you think are relevant to assessing 'seriousness' of harm?*

Summary of consultation responses

i. Justification for use

A consistent theme across responses was that the use of biometric and facial recognition technologies should be exceptional rather than routine and should be clearly justified. Many respondents argued that such technologies should only be used where there is a demonstrable operational need and where less intrusive methods would be ineffective. Some respondents opposed the use of facial recognition and related technologies in any circumstances, citing concerns about accuracy, bias and broader societal impacts. Others accepted limited use, particularly in serious or time-critical situations, provided strong

safeguards were in place. Across these differing views, respondents repeatedly emphasised the importance of clear limits and structured decision-making.

ii. Seriousness of harm

Views were mixed on whether the **seriousness of harm** should be a determining factor in deciding when technologies may be used. Some respondents considered seriousness, particularly where there is imminent risk, to be a relevant consideration. Others argued that seriousness alone is insufficient and could be applied too broadly or subjectively. Respondents raised concerns that relying solely on seriousness could enable mission creep, with technologies justified for increasingly routine purposes. Many respondents therefore stressed that seriousness should be considered alongside other factors, rather than operating as a standalone threshold.

iii. Assessing necessity, proportionality and intrusion

Respondents emphasised that decisions about use should take account of the level of intrusion involved. Factors raised included:

- the scale of deployment and number of people affected
- the setting or location, particularly public spaces where individuals may have limited ability to avoid surveillance
- the impact on non-suspects, bystanders, children and vulnerable individuals, and
- the duration of use and treatment of resulting data.

Concerns about privacy, surveillance and civil liberties were frequently expressed within this context. Rather than always viewing privacy as a separate issue, privacy concerns were often framed as an outcome of insufficient controls on necessity, proportionality and authorisation.

Government response

The Government believes that biometric, facial recognition and similar technologies are valuable tools in tackling serious crime and enhancing public safety but we recognise they should only be used when necessary, proportionate and justified, and that clear rules to support consistent use and adoption of technologies like facial recognition are essential to maintaining public trust. We believe that the seriousness of the crime should not be the sole criterion for assessing whether the deployment of the technologies is necessary and proportionate but instead that it must be considered alongside other factors including the scale and nature of the deployment and the impact on individual rights. The law will require justification according to specific criteria and consideration of detailed guidance.

4. Oversight, safeguards and governance

This section summarises the consultation feedback relating to safeguards, oversight and governance arrangements for the use of facial recognition and other biometric technologies in law enforcement. This theme relates to the below consultation questions:

- *Should some uses require more senior authorisation?*

- *Should independent oversight authorisation be required in some circumstances?*
- *In what circumstances should biometric searches of other government databases be permitted?*
- *If biometric searches take place, what safeguards should be in place?*
- *Should functions be undertaken by a single independent oversight body?*
- *What powers or obligations should the oversight body have?*
- *Should the oversight body set rules to guard against bias and discrimination?*
- *What types of rules might the oversight body be responsible for setting?*

i. Strong expectation of clear safeguards and accountable decision-making

A consistent theme in the consultation feedback was that biometric, facial recognition and similar technologies should operate within a clear and robust legal framework supported by safeguards that are understandable, enforceable, and capable of maintaining public confidence. Respondents, including those otherwise critical of these technologies, frequently framed safeguards as essential to ensuring use remains lawful, proportionate and limited to justified purposes.

ii. Authorisation

Many respondents supported the view that some uses should require more senior authorisation, with approval requirements reflecting the level of intrusiveness and risk. Several consultees argued for a tiered approach, in which higher-risk uses attract higher levels of scrutiny.

A recurring point was that independent oversight should play a meaningful role in the governance of more intrusive uses, particularly where deployments could impact rights, public trust, or involve wider datasets.

iii. Safeguards in practice: transparency, auditability, standards and redress

Across responses, consultees highlighted practical safeguards they considered necessary to make governance effective, including:

- clear operational limits on when and how technologies can be used
- logging and audit requirements for searches and access to datasets
- transparency measures (including meaningful public information)
- systems and procedures to reduce the risk of misidentification and inappropriate action, and
- mechanisms for review, learning, and where relevant, redress.

Respondents also raised repeated concerns about bias, error rates and discrimination, with calls for consistent standards and monitoring to ensure performance is fair across demographic groups and deployment environments. Several respondents noted the importance of standards addressing accuracy, confidence thresholds, and real-world operational conditions, rather than laboratory performance alone.

iv. Oversight models and powers

Views differed on whether oversight functions should sit within a single independent body or across a set of oversight mechanisms. However, consultees broadly supported the proposition that oversight should be independent, effective, and equipped with meaningful powers. Respondents identified a range of oversight functions they considered important, including the ability to:

- set and publish rules, standards or codes of practice
- investigate potential misuse, non-compliance or rights impacts
- require information from law enforcement bodies
- support transparency through reporting and publication, and
- enforce compliance through proportionate measures.

Some respondents also argued that oversight should be able to respond to emerging risks, including new technologies and new uses.

v. Other government databases

Where respondents addressed biometric searches of other government databases, concerns focused on the sensitivity of accessing data collected for other purposes and the risk of expansion beyond original intent. Consultees commonly stressed that, if such searches are permitted, they should be subject to strict statutory criteria, robust authorisation, and strong independent oversight, alongside clear limits on retention and use.

Government response

The Government recognises the clear expectation that the optimal solution must include robust safeguards, effective governance and meaningful oversight as new biometric and overt surveillance technologies are adopted. These elements are essential to ensuring lawful and proportionate use of these technologies and to maintaining public confidence in their use. The Government will create a single oversight body to oversee law enforcement use of biometrics, facial recognition and similar technologies. The design of this body and its relationship with other regulators will take account of the existing roles of the Biometrics and Surveillance Camera Commissioner and the Forensic Science Regulator in England and Wales and seek to ensure a seamless and consistent approach across the functions within its scope. This independent oversight body will be responsible for overseeing compliance with the new statutory rules and obligations, including the statutory Code of Practice. The new body will have enforcement powers to ensure adherence to these rules.

Protecting against bias and discrimination is a key priority for the Government in designing this framework and the legislation will introduce rules ensuring that any technology used is adequately tested, scientifically valid and subject to appropriate monitoring.

The Government recognises that enabling law enforcement authorities to conduct targeted checks against databases operated by non-law-enforcement public authorities may present a higher level of interference with individuals' right to privacy. We will ensure the framework acknowledges this and will continue to subject law enforcement searching of such datasets to limited purposes with clear thresholds and statutory safeguards.

The use of technologies that rely on biometric data should continue to be subject to a strict authorisation process and the legislation will stipulate the minimum rank of police officer (or equivalent) who can give operational authorisation. This approach is consistent with existing safeguards for police powers that interfere with individual rights, for example the requirement under the Police and Criminal Evidence Act 1984 for intimate searches.

5. Other consultation activities

i. Targeted engagement with under-represented groups

Alongside the public consultation, the Government commissioned targeted engagement with specific groups to ensure that views from those less likely to respond to government consultations, but whose trust and confidence are important to the legitimacy of a future framework, were meaningfully included. This work involved participants who were cautious or opposed to police use of facial recognition technology, including people from racially minoritised backgrounds. The engagement took place through deliberative sessions held in London and Manchester.

The engagement was designed to complement the public consultation by providing a richer and more inclusive evidence base. It enabled participants to engage with balanced information about facial recognition technology, consider the Government's proposals, and deliberate on appropriate safeguards and oversight. This approach helped surface perspectives, lived experiences and concerns that are not typically captured, strengthening the robustness of the policy development process.

Summary of responses

The engagement found that participants did not reject police use of facial recognition technology but took a cautious and conditional view. Trust in policing emerged as a central factor shaping acceptability. Participants emphasised the importance of clear legal limits, necessity and proportionality, strong safeguards to address risks such as misidentification, bias and deliberate misuse, transparency about how the technology is used, and independent oversight with meaningful powers. They also suggested that oversight arrangements should include public involvement and representation, including voices from communities most affected. Participants felt that this would help strengthen accountability, reflect local context, and build trust in decisions about when and how facial recognition is used.

Government response

The Government welcomes these findings, which align with the Government's intention to provide greater public assurance and give police forces in England and Wales greater confidence to use facial recognition within a strong and well-defined legal framework. As part of the framework, the Government intends to make public participation in oversight a statutory requirement for both police forces and the new independent oversight body.

The full report of the targeted engagement has been published alongside this response.

Table of definitions

The definitions below are provided for clarity and accessibility and reflect how terms are used for the purposes of this consultation response.

Key terms used in this response

Term	Definition (for the purposes of this consultation response)
Biometric data / biometric technologies	Data and technologies that relate to physical, physiological or behavioural characteristics which can be used to allow or confirm the unique identification of an individual. This includes, for example, facial images, fingerprints and DNA, as well as technologies that analyse these characteristics.
Facial recognition technology (FRT)	Technologies that process facial images to identify or verify an individual's identity, or to assess whether a person's image matches images held within a dataset or watchlist. This includes both live and retrospective uses.
Live facial recognition (LFR)	The real-time processing of facial images captured by cameras to identify individuals of interest by comparing those images against a predefined dataset or watchlist.
Retrospective facial recognition (RFR)	The processing of previously captured images or video footage, such as custody images or recorded CCTV, to identify or verify an individual's identity after an event has taken place.
Inferential technologies	Technologies that analyse biometric or similar data to infer characteristics, attributes or states about an individual, such as emotions, behaviour, intentions or actions, rather than to identify them.
Overt surveillance technologies	Technologies used in a visible and identifiable way, where individuals are likely to be aware that surveillance may be taking place, such as fixed or overtly deployed cameras in public spaces.
Law enforcement organisations	Public authorities with statutory functions relating to policing, the prevention and detection of crime, public order, or safeguarding, including police forces in England and Wales.
Watchlist	A dataset or collection of images against which facial recognition technology is used to identify individuals of interest for a specific and defined purpose.
Oversight	Arrangements designed to provide accountability, scrutiny and assurance that technologies are used lawfully, appropriately and in accordance with applicable rules, safeguards and standards.

3. Impact Assessment, Equalities and Welsh Language

Impact Assessment and Equalities Impact Assessment

Both an equalities impact assessment and an options assessment were published alongside the consultation. The Government will publish a full impact assessment and revised equalities impact assessment when legislation is brought forward to enact the new framework.

Welsh Language Impact Test

In accordance with the Welsh Language Act 1993, the Home Office's Welsh Language Scheme, requires us to 'assess the linguistic consequences of policies affecting services provided to the people in Wales'. The following areas have been considered in the light of responses to the consultation exercise.

- Were there any responses from Welsh stakeholders that raised particular issues or considerations for Wales or Welsh-speakers that need responding to?

No Welsh-language-specific issues were raised in consultation responses.

- If yes, have you assessed the likely impacts on service delivery of the policy proposals on the use of the Welsh language in Wales?

No impacts identified.

- What action have you taken to ensure that the policy proposals are consistent with the requirements set out in the Home Office Welsh Language Scheme? (e.g. have you considered having a Welsh language translation of the consultation response?)

The proposals are linguistically neutral. Welsh translation of the government response has been considered, and existing Welsh-language requirements will continue to apply.

Further guidance can be found here: https://www.gov.uk/government/organisations/home-office/about/welsh-language-scheme

4. Consultation principles

The principles that Government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the Cabinet Office Consultation Principles 2018:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement

Any enquiries regarding this publication should be sent to us at fr-consultation@homeoffice.gov.uk.