Findings from ICO consensual audits on Freedom of Information of police forces in England and Wales

Date issued: July 2024

Information Commissioner's Office

Contents

Introduction

The Information Commissioner's Office (ICO) is responsible for enforcing and promoting compliance with data protection legislation as well as the Freedom of Information (FOI) Act 2000 and Environmental Information Regulations (EIR). Section 47 of the FOI legislation provides provision for the Commissioner to assess whether a public authority is following good practice, including compliance with the requirements of this Act and the provisions of the codes of practice under sections 45 and 46.

Compliance with the FOI and EIR legislation is not only a legal obligation for police forces but also a cornerstone of transparency, accountability, and public trust. The ICO views auditing as a constructive process with real benefits for controllers and aims to establish a participative approach. As part of this approach, we conducted a series of nine consensual audits involving ten police forces (with one being a joint force audit). The objective was to assess the extent to which FOI/EIR accountability, policies and procedures, performance measurement controls and reporting mechanisms to monitor compliance are in place and operational within each organisation. The individual audit reports provided force-specific recommendations to improve compliance with FOI/EIR legislation where non-conformities were identified.

This outcomes report highlights the key findings and shared themes from nine individual audit reports of police forces in England and Wales. It covers audits conducted between July 2023 and March 2024. The report aims to assist police forces in identifying potential areas for improvement in their FOI practices as the recommendation themes apply broadly.

Our approach

Audits were conducted following the Information Commissioner's audit methodology. The key elements of this were a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

The primary purpose of the audits was to provide the ICO and the participating police forces with an independent opinion of the extent to which they are complying with the FOI legislation. The audits also aimed to highlight potential risks to their compliance and reviewed how well organisations demonstrate good practice in discharging their functions under the FOI legislation.

In instances where weaknesses were identified, recommendations were made, primarily aimed at enhancing existing processes to improve compliance with FOI legislation. To help participating police forces implement the recommendations, each recommendation was assigned a priority rating based on the associated risks. These ratings were assigned based on the ICO's assessment of the risks involved. However, as individual police force priorities and risk appetites may

differ, they are encouraged to undertake their own assessments of the identified risks.

We produced individual reports for each participating police force, detailing our audit findings and providing tailored recommendations to strengthen compliance. The executive summaries of those reports were published on the ICO website.

Areas for improvement

From our audit programme, we noted several main areas for improvement that featured in individual, or across several of the participating police forces. These are summarised below along with relevant recommendation themes that we made.

Governance

Issues and recommendation themes in areas of governance were identified in several forces. These related to staffing levels and resource allocation, compliance with FOI statutory timelines, and publication scheme use and effectiveness.

Staffing levels and resource allocation

Several police forces reported resourcing challenges and inconsistent compliance with statutory timescales for responding to FOI requests. Insufficient resources lead to delays in responses and a backlog of requests, potentially undermining transparency, and public trust. Timely information retrieval from departments facing high demand or staffing shortages due to vacancies and staff absences poses a regular challenge. There should be a clear and effective escalation of such issues where the ability to meet statutory timelines for responses is impacted.

A recurring recommendation theme was to emphasise the need for regular review and adjustment of resourcing levels, as necessary, to ensure resources supporting the FOI team are sufficient to:

- respond within the statutory timescales;
- work through any existing backlog; and
- explore opportunities to enhance efficiency of processes.

These recommendations aim to enhance FOI compliance, streamline processes, and allocate resources effectively.

Publication scheme use

Frequent issues identified include the underutilisation of publication schemes and the need to improve them. The FOI legislation not only mandates timely responses to information requests, but also requires every public authority to have an ICO approved publication scheme and to publish information covered by the scheme. Proactive publication schemes enhance transparency and may help reduce the volume of new FOI requests.

Common publication scheme-related recommendations for participating police forces are listed below:

- Document operational procedures for updating the publication scheme to support compliance.
- Ensure there is sufficient oversight of the publication scheme, with clear responsibilities assigned for publishing information.
- Regularly review the publication scheme to ensure relevant information is published proactively.
- Improve the alignment of the publication scheme with ICO guidance[1,2], including the need for more frequent and scheduled releases within the relevant information classes.

Policies and Procedures

A robust framework of policies and procedures is required to support and give direction to staff towards FOI compliance. Recommendations for improvement were made in the following areas:

- FOI/EIR policies and procedures should be comprehensive and formally documented.
- All processes for the handling of FOI/EIR requests should be formally documented in relevant policies or procedures. This includes information such as what a valid FOI request looks like, statutory timeframe for responding, exceptions, redactions, staff training, the internal review procedure and how to conduct and apply the public interest test (PIT).
- FOI processes should include provisions for the treatment of personal information. This will help mitigate the risk of non-compliance with data protection legislation, including inappropriate disclosures.
- Policies and procedures should be reviewed regularly to ensure they remain current and compliant with relevant legislation. They should contain sufficient detail to guide staff in handling requests.
- There is a need for documentation of procedures within the FOI team to prevent knowledge loss and ensure capability continuity. This will ensure the continuity of good practices and provide clear guidance on performing duties.
- Ensure staff are aware of written FOI policies and procedures, including any updates or supporting guidance.
- Mechanisms should be introduced to ensure that staff have had the opportunity to read and confirm their understanding of instructions. This will help to support compliance with handling requests.

---

[1] Publication schemes: a guide | ICO

[2] Definition documents | ICO

- The FOI section of the website should include an email and postal address so individuals have options as to how they can submit written requests, follow up on a pending request or make a complaint.

These findings underscore the need for good documentation, with comprehensive policies and detailed procedures that are easily accessible. Regular reviews are important to ensure that this documentation provide up to date, standardised and organisation-specific guidance for handling FOI requests.

Compliance and Assurance

Areas of compliance and assurance were identified as needing improvement to ensure compliance with statutory requirements and the provision of appropriate responses to requests. The identified areas and our recommendations made to address them, are summarised below.

- There is a consistent need to develop or apply quality assurance (QA) processes that appropriately assess the quality of FOI responses prior to their release (eg via peer review or dip sampling). This is particularly important when personal data is involved in a response and team resources are limited.
- Dip sampling of completed requests should be carried out routinely and documented to ensure that the correct processes are being followed and that exemptions and redactions have been applied correctly. This QA process will help to ensure that responses to requests are appropriate and thorough. It will also allow identification of potential development needs within the FOI team. Any issues with response quality should be fed back to all staff involved in the request process.
- Several police forces were not meeting the statutory timescales for responding to FOI requests at the time of audit. There is a need to address this and resultant backlogs of requests awaiting response.
- Procedures for internal reviews should be documented and made available to all staff. Internal review processes should include checks to ensure compliance with obligations relating to handling complaints as outlined in relevant sections of the codes of practice. This includes sections 45 (request handling), 46 (records management), and 16 (duty to provide advice and assistance).
- In some instances, there was potential for conflict of interest with staff who handle internal reviews having worked on the initial FOI request. To ensure impartiality, internal reviews should be completed by a manager or senior member of staff who was not involved with the original response.

These recommendations highlight the importance of quality assurance, experienced staff oversight, formal documentation of procedures, compliance with statutory timescales, and impartial internal reviews in the compliance and assurance of FOI requests.

Third Party Arrangements

Documented governance arrangements should be in place in instances where the police force works in partnership with other organisations in relation to the handling of requests and/or the management of records. Where this was not in place the following recommendation was made:

- Ensure the process for handling requests, where there are interdependencies with other organisations, is formally documented in a policy or procedure. This will ensure that there is clear guidance for staff on how the relationship is structured and managed in the event of information requests.

Exemptions, Exceptions, and Redactions

We identified common themes relating to opportunities to improve documentation of processes for applying exemptions, exceptions (specifically for EIR) and redactions. It is important not to apply blanket rules for exemptions/exceptions, and to ensure that those responsible for their application are properly trained to do so. Correct application of any redactions is also important. Additionally, we identified quality checks as an area for improvement to ensure the appropriate application of exemptions, exceptions, and redactions. Notably, participating police forces reported receiving very low volumes of requests under EIR.

Recommendations made for these themes are summarised below.

- The processes for applying exemptions and redactions should be formally documented and communicated to staff with responsibilities for FOI.
- As mentioned in the previous section, a formal quality check process should be in place to review the use of exemptions and any resulting redactions prior to release. This can be done through peer review or supervisor quality assurance. When resources are limited, priority should be given to reviewing responses involving personal data.
- Dip sampling should take place on completed requests to assess whether any exemptions and redactions have been applied correctly. A senior staff member or supervisor should complete these checks.

Training and Awareness

Our audits revealed that in some participating police forces, FOI awareness is not sufficiently included in all staff training, which is necessary to support compliance with legislative requirements. Furthermore, not all staff members, particularly those with responsibility for responding to FOI requests, have received role-specific training.

Even amongst those who have received training specific to their role, the training is not always refreshed to maintain current knowledge. Additionally, some police forces do not monitor whether staff have read and understood

policies and procedures. This lack of monitoring extends to FOI training figures, which are not consistently tracked and reported on.

Recommendation themes made to address training and awareness are summarised below.

- All staff should receive induction training that includes general guidance on FOIs such as how to recognise and triage FOI requests. This training should be developed in consultation with Information Governance or equivalent and refreshed at regular intervals.
- Staff with responsibilities for handling FOI requests, both within the FOI team and in departments, should be provided with FOI training suitable to their role. This content should be regularly reviewed and updated as required to reflect changes in legislation and precedent.
- Refresher training within the FOI team should resume for all trained request handlers to ensure that knowledge and practices remain current. Any such refresher training should be documented to help demonstrate commitment to the ongoing development of team members.
- Staff with responsibilities for the handling FOI and EIR requests, including senior staff with significant involvement, should be provided with EIR training suitable to their role. This will ensure their knowledge of the legislation reflects their involvement in the process.
- Existing guidance and reminders for staff should appropriately demonstrate how to recognise FOI/EIR requests. This should include consideration as to how information might be provided to staff beyond the staff intranet and include methods to ensure that staff have read and understood the reminders.
- Training compliance rates should be monitored and reported to relevant governance boards.
- Mechanisms should be in place to provide staff with regular reminders of how to recognise FOI/EIR requests to improve the likelihood of requests being appropriately recognised and appropriately channelled to the relevant team without undue delay.

These themes highlight the importance of comprehensive training and awareness programmes in ensuring FOI compliance.

Personal Data Breach Management and Reporting

Correct handling of any breaches of personal data that occur is essential for an organisation to protect individuals' rights and to meet its legal responsibilities. We found that 50% of police forces audited in this programme had put in place good or reasonable measures to ensure that the team responsible for handling FOI requests is able to effectively detect, assess and respond to personal data breaches that may happen during the handling of an FOI request.

The following recommendations were provided on the theme of personal data breach management and reporting:

- All staff with responsibilities for handling FOI requests should receive personal data breach training. This will ensure that where personal data breaches occur during the handling of an FOI request, staff can address the breach and manage it in accordance with organisational procedure and legislative requirements.
- Refresher training should be provided at appropriate intervals, including how to detect, assess and respond to personal data breaches.
- Personal data breach policies and guidance should be reviewed regularly and updated as required.
- Regular reminders to staff about the processes in place should be considered.

Best practice seen during our audits

From our audit programme we noted areas of good and best practice that either occurred in one organisation or were seen across several organisations. Please note that the area of best practice highlighted below was not present in all the police forces audited.

One best practice observed was the implementation of a weekly risk assessment meeting (RAM). The RAM is an operational platform where all new FOI requests are reviewed and discussed by the FOI team, business area staff responsible for gathering information, and senior officers. The meeting serves to categorise each request as normal, complex or at increased risk of harm if disclosing the information publicly.

The discussions provide useful context for FOI handlers who will prepare responses, and help to determine whether it will be feasible to gather the requested information within the required timeframe. The meeting also identifies the schedule of FOI draft responses that will go to chief officers for review and sign-off. As such, the RAM is a proactive measure that ensures thorough risk assessment and appropriate handling of all FOI requests.

This practice has proven to be effective in managing FOI requests. It underscores the importance of transparency, accountability, and risk management. The ICO considers this proactive cross-organisation assessment of FOI requests to be a best practice and encourages its wider adoption.

Recommendations made in our audits

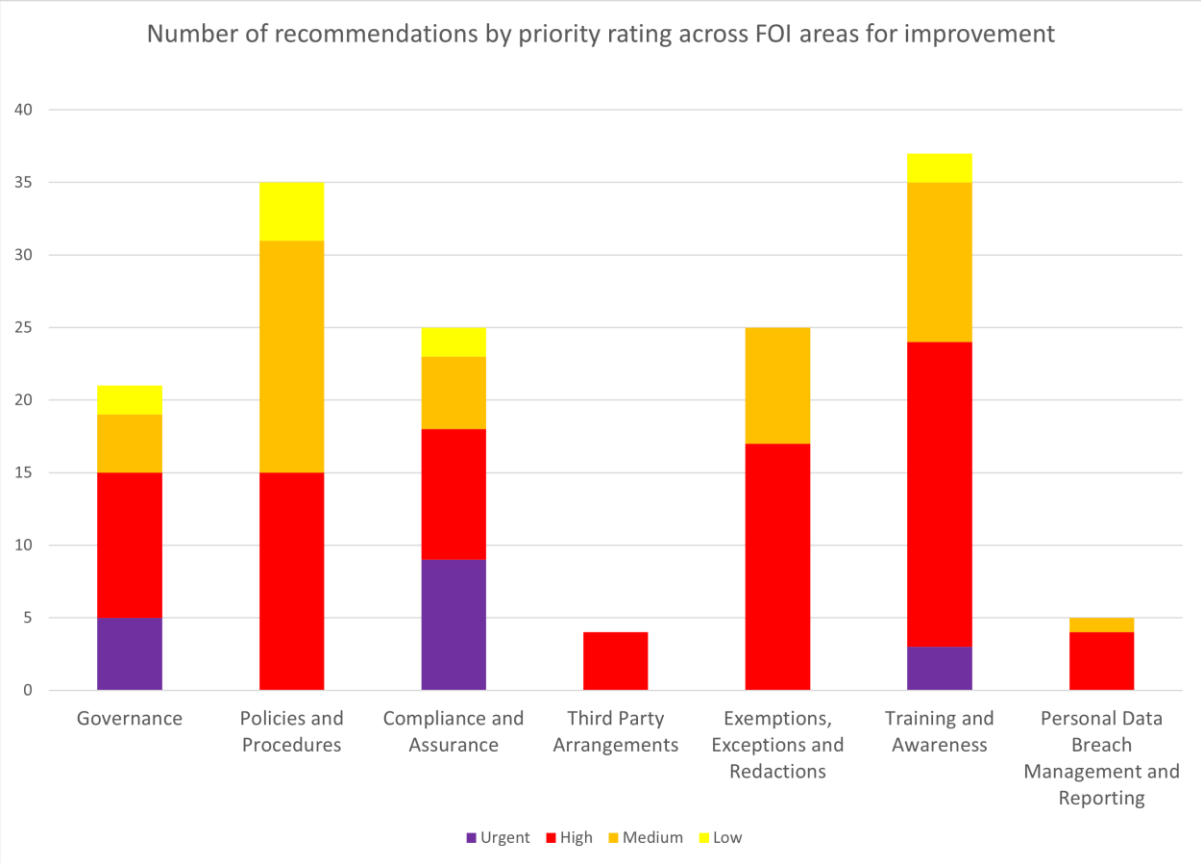
Each individual police force audited received an overall assurance rating as to the extent to which processes and procedures are in place and are delivering FOI compliance: high, reasonable, limited or very limited. The overall assurance

ratings provided during the audit programme along with their descriptions are summarised in Appendix 1.

Where we identified areas of non-conformity, we made specific recommendations to assist the police forces in addressing them.

All recommendations were assigned a priority rating to indicate the risk to FOI compliance if they were not implemented: urgent, high, medium, or low. Appendix 2 shows the priority rating descriptions in detail.

We made 152 recommendations across the nine audits. Of these, 17 (11%) were assessed as urgent and 80 (53%) were assessed as high priority. These were distributed across the areas for improvement covered earlier in this report and as shown in the bar chart.

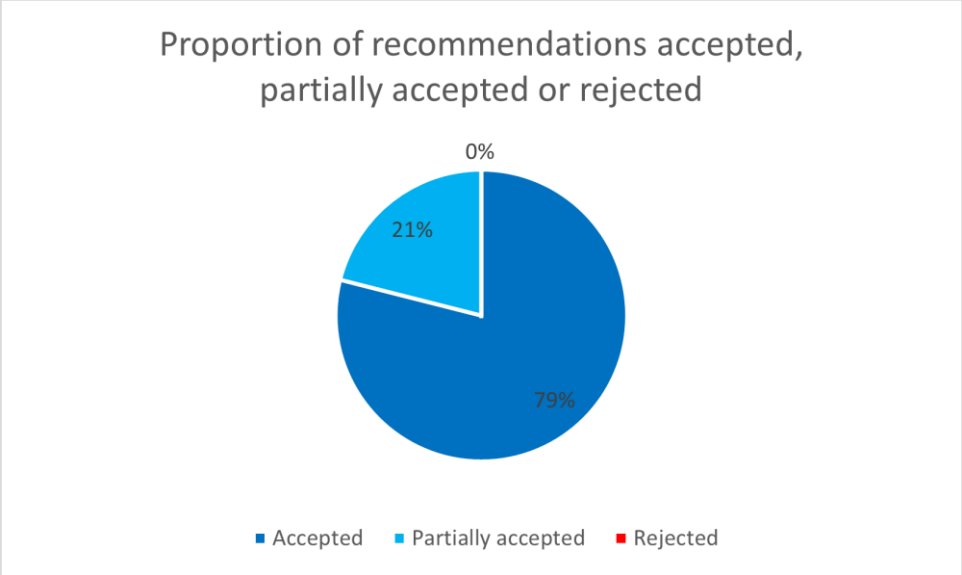


A total of 17 recommendations were assigned an urgent priority, distributed across the areas of:

- Compliance and Assurance (9);
- Governance (5); and
- Training and Awareness (3).

Of the 80 recommendations assigned a high priority, most were distributed across the areas of:

- Training and Awareness (21);
- Exemptions, Exceptions and Redactions (17);
- Policies and Procedures (15); and
- Compliance and Assurance (9).



79% (120) of the ICO audit recommendations were fully accepted by participating police forces, 21% (32) were partially accepted, and actions to mitigate the risks were formally documented and agreed. Notably, none of the recommendations were rejected.

Follow-up audits

In addition to the audit reports and recommendations, the ICO will conduct follow-up audits with each participating police force. The purpose of these follow-up audits is to mitigate identified risks, support compliance with FOI legislation and foster good practice.

Each participating police force received a detailed report of our specific audit findings, including recommendations to amend non-compliance or improve practice, where relevant. In response, they each submitted action plans to detail how they intended to address identified non-conformities. Follow-up audits will take place between six to 12 months after the publication of each individual audit report. These follow-up audits will allow the ICO to assess progress made against the agreed action plan. If there are any concerns with progress made, the Information Commissioner will consider whether it is appropriate to exercise his formal enforcement powers to ensure compliance with the FOI legislation.

Conclusion

This audit programme by the ICO has provided valuable insights into the compliance of police forces in England and Wales with the FOI legislation. The audit programme identified several areas requiring improvement, particularly in relation to governance, policies and procedures, compliance and assurance, and training and awareness.

The findings and recommendations in this report, particularly those of urgent and high priority, are intended to serve as a guide for all police forces in England and Wales. They highlight the importance of promptly addressing areas of non-compliance to mitigate risks to FOI compliance. It is crucial for all police forces, regardless of whether they participated in this audit, to regularly review and adjust their resourcing levels, develop comprehensive FOI/EIR policies and procedures, apply quality assurance processes, and provide adequate and appropriate training to all staff.

This report underscores the importance of regular reviews, comprehensive policies and procedures, robust quality assurance processes, and effective training in ensuring FOI compliance. It is our hope that the findings and recommendations of this report will serve as a helpful resource for police forces in their ongoing improvement efforts to uphold transparency, accountability, and public trust.

The ICO would like to express its gratitude to all the participating police forces for their cooperation and commitment to improving their FOI practices. We look forward to seeing the implementation of the recommendations and the subsequent enhancement of FOI compliance across police forces in England and Wales.

Acknowledgements

We would like to thank the following police forces for their participation in this audit programme:

- Devon & Cornwall Police and Dorset Police
- Dyfed-Powys Police
- Humberside Police
- North Yorkshire Police
- South Yorkshire Police
- Leicestershire Police
- Warwickshire Police
- West Mercia Police
- West Yorkshire Police

Appendix 1 – Assurance ratings

Number = number of organisations

Scope Area	High	Reasonable	Limited	Very Limited
Freedom of Information	0	6	3	0

Key:

High: There is a high level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with freedom of information legislation.

Reasonable: There is a reasonable level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

Limited: There is a limited level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with freedom of information legislation.

Very Limited: There is a very limited level of assurance that processes and procedures are in place and are delivering freedom of information compliance. The audit has identified a substantial risk that the objective of freedom of information compliance will not be achieved. Immediate action is required to improve the control environment.

Appendix 2 – Recommendation priority ratings descriptions

Urgent Priority Recommendations These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of freedom of information legislation.
High Priority Recommendations These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of freedom of information legislation.
Medium Priority Recommendations These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.