Information management

Freedom of information

The General Data Protection Regulations (GDPR) and the Law Enforcement Directive (LED) takes effect from 25th May 2018. Work is currently being carried out to ensure that these regulations are reflected here. In the meantime, further information can be found here.

The Freedom of Information Act 2000 (FOIA) provides any person, anywhere in the world the right to access information held by public authorities, subject to a number of exemptions. All police forces are separate public authorities subject to this Act. The FOIA places statutory obligations on public authorities and guidance from the Information Commissioner's Office (ICO) is available to help forces meet those responsibilities. The FOIA interfaces with Data Protection Act 1998 (DPA).

Contents

1 Obligations and responsibilities
- 1.1 Public authorities
- 1.2 NPCC national policing freedom of information and data protection central referral unit
- 1.3 Information Commissioners Office
- 1.4 Forces
- 1.5 Freedom of information officer

2 Freedom of information request process
- 2.1 Information liable for disclosure
- 2.2 Information not liable for disclosure
- 2.3 Requests
- 2.4 Dealing with a request
- 2.5 Fees and charges
- 2.6 Timescales
- 2.7 Responding to the applicant
  - 2.7.1 Internal review and appeals
- 2.8 Vexatious and repeated requests
- 2.9 Transferring the request
  - 2.9.1 Consultation with third parties
- 2.10 Decision making process
  - 2.10.1 Stage 1 – information gathering
  - 2.10.2 Stage 2 – neither confirm nor deny
  - 2.10.3 Stage 3 – harm
  - 2.10.4 Stage 4 – exemptions
  - 2.10.5 Stage 5 – public interest test

3 Freedom of information exemptions
- 3.1 FOIA section 21 – information reasonably accessible by other means
- 3.2 FOIA section 22 – information intended for future publication
- 3.3 FOIA section 23 – information supplied by, or relating to, bodies dealing with security matters
  - 3.3.1 Relationship between section 23 and section 24
- 3.4 FOIA section 24 – national security
  - 3.4.1 Ministerial certificates
- 3.5 FOIA section 27 – international relations
- 3.6 FOIA section 28 – relations within the UK
- 3.7 FOIA section 29 – the economy
- 3.8 FOIA section 30 – investigations and proceedings conducted by the public authority
  - 3.8.1 Historical investigation records
  - 3.8.2 Relationship between FOIA section 30 and 31
- 3.9 FOIA section 31 – law enforcement
- 3.10 FOIA section 32 – court records
- 3.11 FOIA section 36 – prejudicing the effective conduct of public affairs
- 3.12 FOIA section 37 – communication with the royal family and honours
- 3.13 FOIA section 38 – health and safety
- 3.14 FOIA section 39 – environmental information
- 3.15 FOIA section 40 – personal information
- 3.16 FOIA section 41 – information provided in confidence
- 3.17 FOIA section 42 – legal professional privilege
- 3.18 FOIA section 43 – commercial interests
  - 3.18.1 Contracts/confidentiality clauses
- 3.19 FOIA section 44 – prohibitions on disclosure

4 Force publication scheme
- 4.1 Guide to published information
- 4.2 Monitoring and reviewing the force publishing scheme
- 4.3 Complaints procedure

5 Environmental information regulations

Obligations and responsibilities

Public authorities

Police forces and police and crime commissioners (PCCs) are public authorities under FOIA. The FOIA confers two obligations on public authorities:

- the duty to confirm or deny whether the information requested is held
- the duty to communicate the information.

There are two main ways of releasing information:

- disclosure in response to a valid request (subject to exemptions where applicable)
- creating and maintaining a publication scheme.

NPCC national policing freedom of information and data protection central referral unit

The national police freedom of information (FOI) and data protection (DP) central referral unit (CRU), a component of the NPCC, is responsible for:

- providing advice and support on FOI and DP issues to law enforcement agencies
- formulating and developing information rights policy
- encouraging FOI good practice
- maintaining and developing relationships with partner agencies
- managing intelligence in relation to misuse of the legislation
- ensuring national policing leads are able to contribute to information disclosure decisions when they affect the police service
- producing and delivering national FOI and DP training, workshops and professional development events.

Contact details

acpo.advice@foi.pnn.police.uk

08448929010

The CRU provides advice and guidance to forces in order to mitigate risks in statutory compliance in relation to FOI or Environmental Information Regulations 2004 (EIR) requests. In all circumstances, forces must refer requests to the CRU which relate to the following areas of police business:

- protected persons
- requests that name and or relate to information which may originate from any of the FOIA section 23 bodies.

Where information is already not officially published or previously released under FOIA, forces should refer requests on the following topics to the CRU:

- covert operations or surveillance activities
- counter terrorism and/or national security material or operations – including Special Branch, CBRN and port/airport operations
- VIP/royalty protection
- national systems, for example, ANPR
- sex offender or dangerous offender management
- national policing guidance
- information received from, or relating to, partner agencies – including national policing, government departments, Independent Police Complaints Commission (IPCC), Crown Prosecution Service (CPS) and College of Policing
- major or complex investigations, operations or incidents – for example, cross border incidents, large scale public disorder, multiple or high profile deaths.

In addition to these mandatory referrals, forces may also refer any requests that require specific disclosure or technical advice.

When a force refers a request to the CRU, it must submit the request on the referral template. Once a force has referred a request for information to the CRU, the force must not answer the request until receiving guidance from the CRU.

Compliance with this process will help mitigate the following risks:

- accidental disclosure of sensitive information
- forced disclosure by the Information Commissioner's Office or information tribunal following the misapplication of the legislation
- disclosures which adversely affect partner agencies, other forces or the police service as a whole
- ill-considered disclosures which lead to the harm of an individual or members of the public
- substantial fines in the case of DPA breaches or enforcement action for poor FOIA compliance
- adverse reputational damage
- loss of public confidence.

Information Commissioners Office

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner can take enforcement actions, which include issuing monetary penalties.

Forces

Chief officers have statutory obligations in relation to the FOIA and will be held to account for breaches of the legislation. All staff are responsible to ensure they comply with the Act. Chief officers are advised to designate FOI officers to coordinate and manage FOI requests made to the force. Any member of the force who believes they have received a request must handle it in accordance with local policies and procedures.

Freedom of information officer

FOI officers are responsible for ensuring organisational compliance with FOIA and FOI unit staff are responsible for administering that compliance.

All FOI unit staff responsible for decision making should have completed the CRU FOI Decision Maker Training. FOI units must have staff vetted to at least SC level and empowered to make information disclosure decisions on behalf of the chief officer.

For further information see:

- Administer compliance with Freedom of Information legislation
- Ensure organisational compliance with Freedom of Information legislation.

Freedom of information request process

Information liable for disclosure

Under the FOIA any information, documentation or records that are created by, or in the possession of a public authority may be covered by the scope of a request and are liable for disclosure. This refers to:

- anything in a permanent recorded format (for example, video, audio recordings, hand written reports, notes, emails, minutes, etc.)
- information in the possession of another body or organisation on the authority's behalf (for example, a records storage company, archive or private contractor).

It is irrelevant who created the information, where it originated or who owns it. Any information which has been created or used in connection with the activities of the authority at the time a request is received is considered held and subject to FOI disclosure. The definitive case law on whether information is held or not is McBride vs ICO and Ministry of Justice (MoJ).

Information not liable for disclosure

Not all information is held for the purposes of FOI. Information not liable for disclosure is information held solely on behalf of another party or body. Examples may include emails sent from the police federation to its members on the force email system, web page histories where staff have used their free time to carry out online shopping, a staff member's private diary (even if it is kept in their office desk).

The status of this type of information can change. An email sent to all officers by the federation but copied into the force for the chief constable's information, now becomes held by the force for a business purpose. Websites visited by staff, in their own time, which become part of a misconduct investigation and even entries in private diaries (if they relate to work appointments) are all events where the status of what is considered held or not held may change during the lifecycle of information.

This is also relevant to the work of chief officers who are coordination committee or national operation leads. Emails and meeting minutes may well be on the force system but they are just holding them on behalf of another body or organisation.

Similarly, the status of chief officer material can change. For example the national coordinator on public order may have created a guidance document as part of their national obligations and typed and saved it on the force system. However, this would not be considered held by the force for the purposes of a FOI request unless, for example, if it was then sent to the force public order department to be implemented. At this point, the document would be held for the purposes of the force's business.

Requests

A FOI request can be made by anyone from anywhere in the world and, provided the request is valid, it must be processed under the legislation by the receiving force. A disclosure made to an applicant under FOI is considered a disclosure to the world and is therefore available to anyone else upon request. Information disclosures outside of FOI do not carry this same obligation.

Non valid requests do not have the same statutory requirement attached to them and do not require legal processing.

Requests do not have to:

- be written on a special form
- mention the FOIA or refer to FOIA in any way.

In terms of a badly worded or noncompliant request, the force should provide some advice and assistance to the applicant in order to make the request valid.

Forces should assess potential requests at the point of receipt into the organisation and the best option for dealing with them. For example, a request for information on the force's website should be responded to immediately with the relevant link, rather than completing a time-consuming bureaucratic process of a response letter being sent, followed by the link in another response several days later.

Some requests are complex and wordy and may contain multiple questions. This sometimes makes it difficult to understand what information is being sought. The applicant should be contacted to seek clarification as to exactly what is required. It may even help to ascertain why they want it. It is acceptable to suggest better questions.

Where it is unclear as to whether it is a FOI request, or it is possible that the applicant is incorrectly using the legislation, the force should contact the applicant and make further enquiries. For example, if someone is requesting information about their crime, this may be better dealt with by the officer in charge (OIC) or under subject access.

If requests are received from another force or partner agency, the force should contact the applicant to ascertain whether they are making a personal request or applying on behalf of the organisation. Organisational requests should be dealt with outside of the legislation as part of normal business. This does apply to union and staff association requests.

Dealing with a request

If the request is valid, the information required has been clearly defined and there is no preferred option for dealing with it outside of the legislation, the force must process it in accordance with the FOIA and the statutory timescales.

Before making a disclosure, the force should ascertain what information is already in the public domain. FOI units should have knowledge of the force website, media releases, the website of the PCC and the publication scheme.

If the information requested is already on an official website or publication then the force should simply direct the applicant to it. It is important to ensure that the published information fully meets the terms of the request and is from an official or verified source. A newspaper or media agency website is not an official source. Forces should not provide media links in order to answer a request (unless it can be verified that it is a verbatim response of the force).

News reports of official events, such as court hearings or police incidents do not mean they are automatically in the public domain. It is possible to breach the DPA and disclose personal data by confirming, under FOIA, that something did or did not happen.

Any information in the public domain, official or not, should be retained within the recorded audit trail of decision making as it may be relevant to public interest later. It would be difficult to explain why material already officially published has now had exemptions applied to it.

Fees and charges

FOIA section 12 provides an exemption from a public authority's obligation to comply with a request for information where the cost of compliance is estimated to exceed the appropriate limit. The option to charge for work in excess of the 18 hours appropriate limit is outlined within the regulations. However, forces cannot be legally compelled to undertake this work and national policing policy is that requests that exceed the limit are refused as these will have serious staff resource implications.

A public authority must still confirm or deny whether it holds the information requested unless the cost of this alone would exceed the appropriate limit.

When estimating the time taken, the force can take the following into account:

- determining if the information is held
- locating the information
- retrieving the information
- extracting the information to be disclosed from the other information.

However, forces cannot consider the following activities when calculating the fees estimate:

- the time spent identifying information to be exempted
- the time dedicated to the process of redaction.

However, forces can consider using FOIA section 14 where this activity would be unduly burdensome.

Timescales

FOIA stipulates that forces should provide a response to a request as soon as practicable, and in any case within 20 working days. If the force cannot immediately reply to a request, they should send an acknowledgement letter containing an estimated end date. Day one of the life of a request is the first full working day after it is received by the force.

Further information

FOIA section 10

It is permissible to have a single extension to this period of 20 working days in limited circumstances. This can only apply when the public interest test cannot be completed within the initial timeframe. This may be due to the information under consideration being highly complex or the need for significant stakeholder engagement. If an extension is required then the force should tell the applicant as soon as possible, together with an outline of which qualified exemption(s) is/are engaged. Any such notice should be worded in such a way to ensure that any future requirement to neither confirm nor deny whether the information is held is not compromised or undermined.

Once the final response is provided, the force must deal with any subsequent request for an internal review within 20 working days.

If a force has requested clarification or asked the applicant for more information in order to process the request, a further 20 working days should be allowed for the applicant to respond before the request is closed. Any correspondence with the applicant should include the end date.

When refusing information, forces must issue applicants with a refusal notice that includes details of how the applicant may make a complaint. They should be allowed 20 working days within which to register a complaint. The deadline for receipt of the appeal should be included in any correspondence. If the applicant comes back with a complaint after the 20 day period, the onus is on the force to determine whether there were any extenuating circumstances to account for the delay (eg, a holiday) before rejecting it. If it is reasonable then the internal review should be allowed.

Where a second request is received for the same or similar information, the interval must be more than 60 working days apart, or else the requests may be classed as repeated and refused under FOIA section 14 (2) or aggregated under FOIA section 12.

Responding to the applicant

When a public authority refuses either to disclose requested information or neither confirm or deny (NCND) that any information is held, it must issue a refusal notice stating the fact of refusal, the exemption(s) used and why it applies. Where qualified exemptions apply, a public authority should make it clear in its refusal notice the public interest factors considered in relation to each separate exemption.

Further information

FOIA section 11

FOIA section 17

A public authority is not obliged to make a statement explaining why NCND is engaged if the statement would involve disclosing information which in itself would be exempt.

Any response should be provided in the format requested by the applicant where it is reasonably practicable to do so.

The force response must include details of how to request an internal review of the force's decision.

Internal review and appeals

If the force receives a complaint, it must provide written acknowledgement to the applicant with an indication of when a response may be expected, which must be within 20 working days.

The internal review stage is an opportunity to consider a request completely afresh. It should be an independent review of the original decision. This process should not be overly bureaucratic. The force must issue a fresh response, compliant with FOIA section 17 if appropriate.

Whatever the result of the review, the force must make the applicant aware of their further rights of appeal to the Information Commissioner's Office. Full contact details for the Information Commissioner's Office must be provided to the applicant.

If the applicant appeals to the Information Commissioner's Office following an internal review, the force must notify the CRU.

Vexatious and repeated requests

Forces do not have to comply with vexatious requests. There is no public interest test and no requirement to provide any information or confirm or deny whether the information is held. In most cases, forces will still need to issue a refusal notice.

A refusal under FOIA section 14(1) must be proportionate and relevant to the circumstances. Forces must retain a full record of the evidence and rationale for the decision.

Applying FOIA section 14(1) is not without risk. FOI unit staff who are unfamiliar with FOIA section 14 or who are dealing with complex cases should contact the CRU for advice and assistance.

There are also provisions for dealing with repeated requests under FOIA section 14(2).

Further information

Information Commissioner's Office Guidance – Dealing with vexatious requests (section 14)

Transferring the request

Requests may be wholly or partially transferred to another public authority, provided the information is not held by the force in receipt of the initial request. This must be done in compliance with the Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000.

For further information see:

- FOIA section 16
- FOIA section 45.

Consultation with third parties

When a third party is affected by disclosure, forces should consult with that third party prior to disclosure, unless consultation is impracticable (for example, because the third party cannot be located or because the cost of consultation is disproportionate). In this case, the police service should consider what is the most reasonable course of action under the requirements of the FOIA and the individual circumstances of the request. If the third party is a national partner agency, consultation can be undertaken on the force's behalf by the CRU.

Decision making process

Once the request has been deemed neither excess cost nor vexatious, there is then a need to make a decision about disclosing the requested information. The decision-making process should start with a presumption of disclosure, but this needs to be assessed on a case-by-case basis depending on the subject matter, the harm identified and the public interest.

There are six potential stages to the decision-making process:

- stage 1 – information gathering
- stage 2 – neither confirm nor deny
- stage 3 – harm
- stage 4 – exemption
- stage 5 – PIT
- stage 6 – refusal.

Stage 1 – information gathering

FOI units need to ascertain what information relevant to the request is held by the force. Information owners have a responsibility to identify information captured by the request and provide access to it for FOI units. Information owners must respond to enquiries from FOI units to ensure organisational compliance with the legislation. The identity of the applicant should not be shared with information owners, or third party stakeholders, unless there is a policing purpose in doing so, for example intelligence gathering. The final decision on whether or not to share the applicant's details will lie with the FOI officer.

It may be possible at this stage to determine that a neither confirm nor deny response may be appropriate.

Stage 2 – neither confirm nor deny

There are obvious situations where confirmation or denial is harmful. For example where confirming the force holds sensitive personal data which would then in itself disclose personal information. There is a need to consistently apply NCND in order that its future use does not cause issues. This is often referred to as the NCND principle.

The application of the NCND principle in terms of FOIA section 1(1)(a) removes the legal obligation to then comply with FOIA section 1(1)(b). If an absolute exemption or the public interest, in terms of qualified exemption, upholds the right to NCND there is no need to further consider the request in terms of disclosure. Consideration should be given to whether the use of NCND is appropriate not just when information is held and but also when it is not.

Failing to abide by the principle can either cause problems with future requests or may handicap other forces or bodies who wish to apply the NCND, but are now restricted because the principle has been compromised by a disclosure made by another force.

There can also be circumstances where a partial NCND is engaged. A force may confirm that some information is held (this may be supplied or exempted) but to confirm that this represents all the information in the possession of the authority would in itself be harmful. This more commonly occurs with the use of exemptions FOIA section 23 and section 24.

Applying NCND is complex and not without risk. FOI unit staff who are unfamiliar with NCND or who are dealing with complex cases should contact the CRU for advice and assistance.

Stage 3 – harm

Potential harm in disclosure should be focused on identifying:

- any stress, mental anguish, fear, physical suffering that could be imposed upon individuals or the public as a whole
- damage to policing in terms of investigation data, tactics, morale, resources, partnership working or public confidence
- national security, UK infrastructure or any commercial interest.

If there is no harm in confirming or denying that information is held, the FOI unit must identify whether any harm would result from disclosing that information.

Where the FOI unit deems it appropriate, information owners and stakeholders must contribute to this stage of the process.

Although harm need not be substantial it must be real, likely and not merely perceived. FOI units must be prepared to challenge the evidence provided, carry out research and record their findings.

Stage 4 – exemptions

If harm in disclosure has been identified then it needs to be linked to the relevant exemption.

Once all the relevant exemptions have been identified as being engaged then they should be filtered and strategic decisions taken on the most suitable ones to apply. This is a technical process and only FOI units, or trained staff, should undertake this.

Stage 5 – public interest test

Once a decision had been made on what exemptions are to be used, forces need to consider if a public interest test (PIT) on disclosure is required. This will depend on whether or not the exemption is 'qualified' or not. Even if exemptions are engaged, the information must still be disclosed unless the public interest in maintaining the exemption is greater than the public interest in disclosing it.

The public interest is not what the public may find interesting. There must be some tangible benefit to the community in such a disclosure.

The PIT factors favouring non-disclosure are generally the same as those established during the harm stage. The FOI unit should identify the positives that may be derived from disclosure.

The PIT factors must relate to the actual information requested on a case-by-case basis. Forces should collate all the positive and negative public interest factors. Forces also need to conduct a balance test to determine whether the information should be withheld.

If any positives and negatives are equally balanced, then it is clear in the legislation that the information must be disclosed.

Freedom of information exemptions

Within the FOIA there is a presumption of disclosure. However, not all policing information is suitable for release and the right to know does not extend to the right to know everything. As a result, the FOIA makes provision for withholding information in certain circumstances when exemptions may be applied.

Applying exemptions to refuse an applicant's right to information is complex as there are four categories of exemptions, and each places different responsibilities on the force to ensure compliance with its statutory obligations:

- absolute
- qualified
- class based
- prejudice based.

The FOIA has the following exemptions that may apply to the police:

- FOIA section 21 – information reasonably accessible by other means
- FOIA section 22 – information intended for future publication
- FOIA section 23 – information supplied by, or relating to, bodies dealing with security matters
- FOIA section 24 – national security
- FOIA section 27 – international relations
- FOIA section 28 – relations within the UK
- FOIA section 29 – the economy
- FOIA section 30 – investigations and proceedings conducted by the public authority
- FOIA section 31 – law enforcement
- FOIA section 32 – court records
- FOIA section 36 – prejudicing the effective conduct of public affairs
- FOIA section 37 – communication with the royal family and honours
- FOIA section 38 – health and safety
- FOIA section 39 – environmental information
- FOIA section 40 – personal information
- FOIA section 41 – information provided in confidence
- FOIA section 42 – legal professional privilege
- FOIA section 43 – commercial interests
- FOIA section 44 – prohibitions on disclosure.

The following exemptions cannot be applied by forces:

- FOIA section 26 – defence (Information Commissioner's Office guidance on Freedom of Information Act Awareness Guidance No. 10)
- FOIA section 33 – audit functions (Information Commissioner's Office guidance on Public audit functions (section 33))
- FOIA section 34 – parliamentary privilege (Information Commissioner's Office guidance on Parliamentary privilege (section 34))
- FOIA section 35 – formulation of government policy and other governmental interests (Information Commissioner's Office guidance on Government policy (section 35)).

FOIA section 21 – information reasonably accessible by other means

In order to reduce bureaucracy, forces should not apply this exemption where requests are received and the information is publicly available on an official website and the link can easily be provided.

For further information see:

- FOIA section 21
- Information Commissioner's Office guidance on information reasonably accessible to the applicant by other means (section 21).

FOIA section 22 – information intended for future publication

Forces should consider creating a FOI publication strategy when dealing with high profile or major incidents. An effective strategy may reduce the impact of FOI requests linked to the event and allows the force to manage disclosure. SIOs in conjunction with their FOI units should consider the strategy at an early stage.

Forces should obtain advice and assistance from CRU.

For further information see:

- FOIA section 22
- Information Commissioner's Office guidance on the exemption for information intended for future publication.

FOIA section 23 – information supplied by, or relating to, bodies dealing with security matters

Forces considering using this exemption or dealing with FOIA section 23 material must refer the case to the CRU.

Examples of when FOIA section 23 exemptions could be applied:

- information from or relating to Special Branch or counter terrorism units (confirmed in Information Commissioner's Office DN FS50488435)
- information on police tactics, when security bodies may work closely with the police to gather intelligence
- policing activities involving the National Crime Agency.

For further information see:

- FOIA section 23
- Information Commissioner's Office guidance on security bodies (section 23)
- Information Commissioner's Office guidance on using Section 23 and 24 in the alternative
- Information Commissioner's Office DN FS50526415.

Relationship between section 23 and section 24

FOIA section 23 and section 24 are mutually exclusive and cannot be applied to the same information except in a NCND scenario. However, uniquely for these two exemptions, it is possible to apply them simultaneously in the alternative. The substantive application in the alternative informs that the exemptions are being relied on, but the public authority is not obliged to confirm which. An example of Information Commissioner's Office support of its use can be found here.

FOIA section 24 – national security

Forces considering using this exemption or dealing with FOIA section 24 material must refer the case to the CRU.

Examples of when FOIA section 24 exemptions could or should not be applied:

- activities or material relating to Special Branch and counter terrorism units (Information Commissioner's Office DN FS50488435)
- counter terrorism grants, costs or prevent, channel, etc.
- covert policing, tactics and surveillance (Information Commissioner's Office DN FS50503055)
- relationships and cooperation between the UK and other countries to include safeguarding of potential targets (Information Commissioner's Office DN FS50469024)
- Royalty/VIP protection and ministerial engagements (Information Commissioner's Office DN FS50406024).

FOIA section 23 and 24 can be applied in the alternative.

Further information

FOIA section 24

Information Commissioner's Office guidance on safeguarding national security – (Section 24)

Information Commissioner's Office guidance on how sections 23 and 24 interact

Tribunal Service Appeal, FOIA – 2007 National Security [IT EA/2006/0045]

Information Commissioner's Office DN FS50490615

Ministerial certificates

Occasionally at an Information Commissioner's Office appeal or information tribunal, it may be necessary to consider the use of a ministerial certificate for section 23 and section 24 exemptions.

This is a complex and highly sensitive process and will be led by the CRU in close consultation with the Ministry of Justice (MOJ) and relevant stakeholder agencies. Forces should seek further information from the CRU.

FOIA section 27 – international relations

FOIA section 27 (1) and section 27(2) exemptions will be used in limited circumstances and with particular reference to forces with international responsibilities or that have relationships with forces overseas.

For further information see:

- FOIA section 27
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No. 14 International Relations.

FOIA section 28 – relations within the UK

This exemption will have limited relevance to the police service.

For further information see:

- FOIA section 28
- Information Commissioner's Office Freedom of Information Act Awareness guidance 13 Relations within the UK.

FOIA section 29 – the economy

This exemption will have limited relevance to the police service.

For further information see:

- FOIA section 29
- Information Commissioner's Office Freedom of Information Act Awareness guidance 15 The economy.

FOIA section 30 – investigations and proceedings conducted by the public authority

It has been established that the police service cannot use the exemptions provided by FOIA sections 30(1)(b) and 30(1)(c). For further information see:

- FOIA section 30
- Information Commissioner's Office guidance on Investigations and proceedings (section 30)
- Information Commissioner's Office DN 50460785.

Historical investigation records

A historical record is one over 30 years old (from the last addition to the record) and it cannot be exempt under FOIA section 30(1). The Constitutional Reform and Governance Act 2010 is reducing this time period to 20 years using a phased approach. Over 10 years from the end of 2013, the time limit is 29 years reducing one year every year, until it reaches 20 years at the end of 2022.

Information relating to criminal investigations held in an historical record could still engage FOIA section 31(1)(a)(b).

For further information see:

- FOIA section 63 as amended by Constitutional Reform and Governance Act 2010 section 46.

Relationship between FOIA section 30 and 31

Where FOIA section 30(1)(a) applies FOIA section 31(1)(a) and 31(1)(b) cannot be used. Forces should consider this when analysing investigation material subject to a request. All the information may not be covered by FOIA section 30(1)(a) as there needs to be a link between the information and the investigation. For example, a crime file may contain a policy or procedural reminder on its completion and this would not be information held for the purposes of a specific investigation, therefore engaging FOIA section 31(1)(a) or 31(1)(b), FOIA section 31(1)(b) instead, if the disclosure would prejudice law enforcement.

FOIA section 31 – law enforcement

Although FOIA sections 30 and 31 are mutually exclusive, they can both be applied in an NCND scenario. For further information see:

- FOIA section 31
- Information Commissioner's Office guidance on law enforcement (section 31).

FOIA section 32 – court records

This exemption will have limited relevance to the police service. For further information see:

- FOIA section 32
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No 9 Information contained in court records
- Information Commissioner's Office DN FS50461639.

FOIA section 36 – prejudicing the effective conduct of public affairs

Information is exempt from disclosure if, in the reasonable opinion of a qualified person (a chief constable or commissioner only), its disclosure would prejudice, or would be likely to prejudice, certain specified interests relating to public affairs.

This exemption will have limited relevance to the police service because the PIT often favours disclosure (Information Commissioner's Office v the CC of Surrey Police (EA/2009/0081)).

For further information:

- FOIA section 36
- Information Commissioner's Office guidance on prejudicing the effective conduct of public affairs (section 36).

FOIA section 37 – communication with the royal family and honours

This exemption will have limited relevance to the police service. For further information see:

- FOIA section 37
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No 26 Communications with Her Majesty and the Awarding of Honours.

FOIA section 38 – health and safety

Forces should take care in using this exemption as it is one of the weakest exemptions due to the amount of evidence that is required to satisfy the Information Commissioner's Office of its suitability.

The definitive case on the level of proof required is People for the Ethical Treatment of Animals Europe Vs the Information Commissioner and The University of Oxford.

The behaviour of the applicant can be taken into account after the request has been made.

For further information see:

- FOIA section 38
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No. 19 Health and Safety
- People for the Ethical Treatment of Animal Europe v Information Commissioner's Office and the University of Oxford (EA/2009/0076)
- Steven Hepple v Information Commissioner's Office and Durham County Council (EA/2013/0168).

FOIA section 39 – environmental information

Where a request for environmental information is made, forces should consider it under the Environmental Information Regulations 2004 (EIR) rather than under the FOIA. For further information see:

- FOIA section 39
- Information Commissioner's Office website – EIR
- Environmental Information Regulations 2004.

FOIA section 40 – personal information

The interface between the DPA and FOIA is complex. Once it has been established that the request is not subject access, practitioners must always determine whether disclosure is fair to the data subject.

For further information see:

- FOIA section 40
- Information Commissioner's Office guidance on Personal information (section 40 and regulation 13)
- Information Commissioner's Office guidance on Requests for personal data about public authority employees
- Information Commissioner's Office guidance Neither confirm nor deny in relation to personal data.

FOIA section 41 – information provided in confidence

Forces should take care in using this exemption. The application of this exemption is complex and requires advice from the force legal services department or the CRU.

For further information see:

- FOIA section 41
- Information Commissioner's Office Freedom of Information Act Awareness guidance 2 Information provided in confidence
- Information Commissioner's Office guidance Freedom of Information Act – The duty of confidence and the public interest.

FOIA section 42 – legal professional privilege

Where FOIA section 42 is being considered or cited, the force's legal services department must be contacted and their views sought.

Prosecution advice obtained from the CPS is not covered by this exemption.

For further information see:

- FOIA section 42
- Information Commissioner's Office guidance on the exemption for legal professional privilege (section 42).

FOIA section 43 – commercial interests

Forces should consult third parties likely to be affected by the disclosure of commercial information to determine likely prejudice. It is not sufficient for the force to speculate about harm. It is the responsibility of the force to decide whether or not the exemption applies, taking into account the views of the third party. However, the third party cannot dictate what is to be exempted.

For further information see:

- FOIA section 43
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No. 5 – Commercial Interests.

Contracts/confidentiality clauses

During the procurement process, suppliers may request forces to sign confidentiality clauses to prevent the disclosure of information. Blanket clauses that are designed to restrict the disclosure of any information, including that which could be disclosed without any prejudice to the commercial interests of the supplier, are not acceptable.

Information created by staff employed by any contractor, on the forces behalf, would be held by the force for the purposes of FOIA.

FOIA section 44 – prohibitions on disclosure

Under this exemption, information is exempt from disclosure if it is prohibited from being released under any other enactment or would constitute contempt of court.

For further information see:

- FOIA section 44
- Information Commissioner's Office Freedom of Information Act Awareness Guidance No. 27 – Prohibitions on Disclosure
- Regulation of Investigatory Powers Act 2000 section 19
- Sexual Offences (Amendment) Act 1992 section 1.

Force publication scheme

The Information Commissioner's Office has produced a model publication scheme that must be adopted by forces. This is an integral part of FOIA compliance. A police sector specific definitions document has been created by the Information Commissioner's Office that must be adhered to.

The CRU has produced a guidance document (National Policing Guide to Publication Scheme Compliance V4.0), endorsed by the Information Commissioner's Office which provides an interpretation of this definitions document and contains the minimum requirements for compliance.

Further information

Information Commissioner's Office – Publication Scheme Guidance

Guide to published information

Each force must produce and publish its own unique copy of the guide that is force specific. The guide will specify:

- the information it will routinely make available (based on the police sector definitions document and the CRU minimum information document)
- how the information can be assessed
- whether a charge will be made for the information requested.

Monitoring and reviewing the force publishing scheme

Forces are required to review the information published under the scheme. The FOI officer is responsible for introducing and maintaining a process to ensure force compliance.

The department owning the information is responsible for ensuring accurate and up to date information is made available.

Complaints procedure

Information on a force web site should include details of how to make a complaint about how the force is operating its publication scheme.

Environmental information regulations

These regulations provide public access to environmental information held by public authorities. The main differences between the EIR and the FOIA are:

Further information

Environmental Information Regulations 2004 (EIR)

- EIR requests may be received verbally and there is no legislative requirement for them to be written down
- the PIT applies to most of the EIR exceptions (regulation 12(3) (personal data of a person other than the applicant) is not subject to the public interest test)
- pseudonyms can be used when submitting an EIR request
- there are exceptions to disclose in relation to internal communications
- exceptions on disclosure where release would adversely affect intellectual property rights or the protection of the environment (under EIR there are no exceptions that link the release of information with a prejudicial impact on the economic interests of the UK or part of the UK)
- an EIR applicant has 40 working days to appeal any decision made by the authority and the authority must respond to any complaint within 40 working days
- EIR do not stipulate a requirement to adopt and maintain a publication scheme although there is a requirement to proactively publish this information.

Page last accessed 06 June 2018

First published: 27 May 2015 **Last modified:** 24 May 2018