Freedom of information

This page is from APP, the official source of professional practice for policing.

First published 27 May 2015 Updated 22 April 2024
Written by College of Policing
29 mins read

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 the **Data Protection Act 2018 (DPA)**.

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 police freedom of information and data protection central referral unit (NPFDU)

The national police freedom of information and data protection central referral unit (NPFDU), a component of the **National Police Chiefs' Council (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

The NPFDU 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.

Contact details:

- **npcc.advice@cru.pnn.police.uk**
- 01489 569826

Information Commissioner's 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 NPFDU FOI Decision Maker Training. FOI units must have some 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 in scope under FOI

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)
- 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. **Definitive case law can be found here**.

Information not in scope under FOI

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 UNISON 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 UNISON 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. The FOIA and the EIR apply to information held by the public authorities and there is no requirement to create new information in order to respond to a request.

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. Go to **Section 16 – advice and assistance** for more information.

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 as a **subject access request (SAR)** under data protection legislation.

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. Force or partner agency 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 s 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 s 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.

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 time frame.

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 40 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 40 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 (for example, 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 suggested interval can be more than 60 working days apart, or else the requests may be refused under **FOIA s 14(2)** or aggregated under **FOIA s 12**.

For further information see **FOIA s 10**.

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.

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.

For further information see:

- **FOIA s 11**
- **FOIA s 17**

How to disclose information safely

When considering the format in which to disclose information, forces should ensure that only the requested information is being provided and that there is no additional hidden data within the document.

Best practice for FOI units is to extract any information provided by business areas into another document, such as a new Microsoft Word or Excel file. Forces should not include the original source spreadsheet within responses to FOI requests.

Officers and staff should avoid disclosing data in the form of Excel spreadsheets or pivot tables. Instead, they should export the data using the comma-separated values (CSV) file format, which only includes visible text. For charts, exporting the document into PDF format will remove the underlying data.

If FOI units do choose to provide information in Excel spreadsheets, they should take extreme caution to ensure that responses do not include hidden data. Hidden data is not immediately visible on the screen, but is held within the file – for example, in hidden rows or columns, which can be easily unhidden and viewed. Other examples of hidden data include hiding entire workbooks or using password protection, neither of which are considered best practice.

Pivot tables, whether created in Excel or in other software, can also contain hidden data. A pivot table can be used to summarise a large set of data housed in other worksheets. Although this hidden data may not be visible within the response and may even be deleted from the workbook entirely, the underlying data may be copied across and accessed via a simple double-click. The same applies to disclosure of information in charts. Depending on how a chart is created, the underlying data may still be retrievable via double-clicking on the chart.

All officers and staff who deal with FOI responses are recommended to ensure that:

- they fully understand their obligations and **ICO guidance**, in respect of removing personal data from information requests and datasets
- original source spreadsheets are not uploaded to online platforms that are used to respond to FOI requests
- all FOI responses containing Excel spreadsheets are reviewed before release, to confirm that no hidden data is contained within the files
- for any FOI request relating to personal data, there is a final double-check of any disclosure by another member of the team

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 s 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 NPFDU.

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

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

For further information, go to **Information Commissioner's Office Guidance – Dealing with vexatious requests (s 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 **Freedom of Information Code of Practice (2018)**.

For further information, see:

- **FOIA s 16**
- **FOIA s 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 NPFDU.

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 – neither confirm nor deny**
- **stage 2 – information gathering**
- **stage 3 – harm**
- **stage 4 – exemption**
- **stage 5 – PIT**
- **stage 6 – response**

Stage 1 – neither confirm nor deny (NCND)

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 s 1(1)(a) removes the legal obligation to then comply with FOIA s 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. It is not a requirement to find out if the information is held by your force in order to apply the NCND.

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 s 23** and **s 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 NPFDU for advice and assistance.

Stage 2 – 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**.

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 has 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.

Stage 6 – response

To comply with **s17 of the Act**, a response letter must be drafted. This can be extremely technical where exemptions are being applied or where an NCND response is required.

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

- **FOIA s 43 – commercial interests**.
- **FOIA s 44 – prohibitions on disclosure**.

The following exemptions cannot be applied by forces.

- FOIA s 26 – **defence (Information Commissioner's Office guidance on Freedom of Information Act)**.
- FOIA s 33 – **audit functions (Information Commissioner's Office guidance on Public audit functions (s 33))**.
- FOIA s 34 – **parliamentary privilege (Information Commissioner's Office guidance on Parliamentary privilege (s 34))**.
- FOIA s 35 – formulation of government policy and other governmental interests (**Information Commissioner's Office guidance on Government policy (s 35)**.

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

FOIA s 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 NPFDU.

For further information see:

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

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

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

Examples of when FOIA s 23 exemptions could be applied include:

- **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 s 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 s 23 and s 24

FOIA s 23 and s 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 s 24 – national security

For further information see:

- **FOIA s 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**

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

Examples of when FOIA s 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 sections 23 and 24 can be applied in the **alternative.**

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 s 23 and s 24 exemptions.

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

FOIA s 27 – international relations

FOIA s 27(1) and s 27(2) exemptions will be used in limited circumstances and with particular reference to forces with international responsibilities (such as training) or that have relationships with forces or other international organisations overseas.

For further information see:

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

FOIA s 28 – relations within the UK

This exemption will have limited relevance to the police service.

For further information see:

- **FOIA s 28**
- **Information Commissioner's Office Freedom of Information Act Relations within the UK**

FOIA s 29 – the economy

This exemption will have limited relevance to the police service.

For further information see:

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

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

It has been established that the police service cannot use the exemptions provided by FOIA s 30(1)(b) and s 30(1)(c).

For further information see:

- **FOIA s 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 s 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 s 31(1)(a)(b).

For further information see:

- **FOIA s 63** as amended by **Constitutional Reform and Governance Act 2010 s 46**

Relationship between FOIA s 30 and s 31

Where **FOIA s 30** applies, **s 31(1) and s 31(2)** cannot be used. Forces should consider this when analysing investigation material subject to a request. All the information may not be covered by FOIA s 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 this would engage FOIA s 31(1)(a) or s 31(1)(b), if the disclosure would prejudice law enforcement.

FOIA s 31 – law enforcement

Although FOIA s 30 and s 31 are mutually exclusive, they can both be applied in an NCND scenario.

For further information see:

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

FOIA s 32 – court records

This exemption will have limited relevance to the police service.

For further information see:

- **FOIA s 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 s 36 – prejudice to 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 see:

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

FOIA s 37 – communication with the royal family and honours

This exemption will have limited relevance to the police service.

For further information see:

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

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

FOIA s 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. The attached link provides further information on the **Data Protection Principles**.

For further information see:

- **FOIA s 40**
- **Information Commissioner's Office guidance on Personal information (s 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 s 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 NPFDU.

For further information see:

- **FOIA s 41**
- **Information Commissioner's Office Information provided in confidence (Section 41) Freedom of Information Act**

FOIA s 42 – legal professional privilege

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

FOIA s 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 s 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 a force's behalf, would be held by the force for the purposes of FOIA.

FOIA s 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 s 44**
- **Information Commissioner's Office Freedom of Information Act Awareness Guidance No. 27 – Prohibitions on Disclosure**
- **Investigatory Powers Act 2016**
- **Sexual Offences (Amendment) Act 1992 s 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 NPFDU has produced a guidance document (**National Policing Guide to Publication Scheme Compliance V5.0**), which provides an interpretation of this definitions document and contains the minimum requirements for compliance.

For further information see:

- **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 NPFDU minimum information document)
- how the information can be assessed
- whether a charge will be made for the information requested

Monitoring and reviewing the force publication 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:

- EIR requests may be received verbally and there is no legislative requirement for them to be written down – the response must always be given in writing (such as an email) regardless of how the response was received
- 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) – **see further information here**
- pseudonyms can be used when submitting an EIR request
- there are exceptions to disclose in relation to internal communications
- there are 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

For further information, go to **Environmental Information Regulations 2004 (EIR)**.

Tags

Information management