

NPCC Manual of Guidance

Freedom of Information Act (2000)

Version 8.1
January 2025

**This manual is fully disclosable under FOI requests.
Please destroy all previous copies of this manual and
work only from this one.**

**If you have a technical FOIA enquiry please check this
manual before contacting the NPFDU.**

**An electronic version of this manual is available on the
Knowledge Hub.**

**Enquiries concerning this manual should be directed to the National
Police Freedom of Information and Data Protection Unit**

****S31(1)****

LIST OF ABBREVIATIONS

ACPOS	Association of Chief Police Officers of Scotland
BAU	Business as Usual
CHIS	Covert Human Intelligence Source
CPIA	Criminal Procedures and Investigation Act
CPS	Crown Prosecution Service
CRU	Central Referral Unit
DDA	Disability Discrimination Act
DP	Data Protection
DPA	Data Protection Act
EIR	Environmental Information Regulations
FOI	Freedom of Information
FOIA	Freedom of Information Act
S23(1)	**S23(1)**
GPMS	Government Protective Marking Scheme
HMIC	His Majesty's Inspector of Constabularies
IC	Information Commissioner
ICO	Information Commissioner's Office
IPCC	Independent Police Complaints Commission (replaced by IOPC)
IOPC	Independent Office for Police Conduct (formally IPCC)
IPCO	Investigatory Powers Commissioner's Office
IT	Information Tribunal
MOG	Manual of Guidance
MOJ	Ministry of Justice
S23(1)	**S23(1)**
NCND	Neither Confirm Nor Deny
NIP	Notice of Intended Prosecution
NPCC	National Police Chiefs Council
NPFDU	National Police Freedom of Information and Data Protection Unit
NSAP	National Security Appeals Panel
PIT	Public Interest Test
PNC	Police National Computer
RAR/ROAR	Right of Access Request (formally SAR)
SAR	Subject Access Request (replaced by ROAR)
SRP	Safer Roads Partnership

USEFUL LINKS

FOIA - [Freedom of Information Act 2000 \(legislation.gov.uk\)](https://www.legislation.gov.uk) [Freedom of Information Act 2000](https://www.gov.uk)
 FOI CODE OF PRACTICE - [Freedom of Information Code of Practice - GOV.UK \(www.gov.uk\)](https://www.gov.uk)
[Freedom of Information Code of Practice - GOV.UK](https://www.gov.uk)
 ICO - [Information Commissioner's Office \(ICO\)](https://www.ico.org.uk)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS	3
USEFUL LINKS	3
TABLE OF CONTENTS	4
FOREWORD	6
INTRODUCTION	7
POLICE SERVICE REFERRAL CRITERIA	8
MANDATORY REFERRALS	10
FOI - THE BASICS	11
EIR	12
PRE-DECISION MAKING	13
○ Is it a valid request?	13
○ Business as usual	14
○ Is the information held?	15
○ Is the information in the public domain?	16
○ Identifying harm	16
SECTION 9 - FEES	18
SECTION 10 - COMPLIANCE	20
SECTION 11 - MEANS OF COMMUNICATING THE INFORMATION	23
SECTION 11A & 11B - DATASETS	26
○ Disclosing Information safely	28
○ ICO Checklist for safe disclosure	30
SECTION 12 - COST OF COMPLIANCE	31
SECTION 13 - FEES FOR DISCLOSURE	34
SECTION 14 - VEXATIOUS REQUESTS	35
SECTION 16 - DUTY TO PROVIDE ADVICE AND ASSISTANCE	39
SECTION 17 - REFUSING A REQUEST	41
SECTION 19 - PUBLICATION SCHEMES	43
NCND	46
INTERNAL REVIEW PROCESS	51
○ Checklist	53
THE PUBLIC INTEREST TEST	55
○ Exemptions requiring a PIT	59
○ Consideration that are invalid	61
FOI EXEMPTIONS	63
SECTION 21 - INFORMATION REASONABLY ACCESSIBLE BY OTHER MEANS	64
SECTION 22 - INFORMATION INTENDED FOR FUTURE PUBLICATION	67
SECTION 22A - RESEARCH	69
SECTION 23 - INFORMATION SUPPLIED BY, OR CONCERNING, CERTAIN SECURITY BODIES	70

SECTION 24 - NATIONAL SECURITY	73
SECTION 26 - DEFENCE	76
SECTION 27 - INTERNATIONAL RELATIONS	78
SECTION 28 - RELATIONS WITHIN THE UNITED KINGDOM	81
SECTION 29 - THE ECONOMY	82
SECTION 30 - INVESTIGATIONS AND PROCEEDINGS CONDUCTED BY PUBLIC AUTHORITIES	83
SECTION 31 - LAW ENFORCEMENT	87
SECTION 32 - INFORMATION CONTAINED IN COURT RECORDS	91
SECTION 33 - AUDIT FUNCTIONS	93
SECTION 34 - DISCLOSURE WHICH WOULD INFRINGE PARLIAMENTARY PRIVILEGE	94
SECTION 35 - FORMULATION OF GOV'MENT POLICY AND OTHER GOVERNMENTAL INTERESTS	95
SECTION 36 - DISCLOSURE PREJUDICING THE EFFECTIVE CONDUCT OF PUBLIC AFFAIRS	97
SECTION 37 - COMMUNICATION WITH THE ROYAL FAMILY AND HONOURS	100
SECTION 38 - HEALTH & SAFETY	102
SECTION 39 - ENVIRONMENTAL INFORMATION	104
SECTION 40 - PERSONAL INFORMATION	105
SECTION 41 - INFORMATION PROVIDED IN CONFIDENCE	110
SECTION 42 - LEGAL PROFESSIONAL PRIVILEGE	114
SECTION 43 - COMMERCIAL INTERESTS	116
SECTION 44 - INFORMATION COVERED BY PROHIBITIONS ON DISCLOSURE	120
 APPENDICES	
APPENDIX 1 ENVIRONMENTAL INFORMATION REGULATIONS	122
APPENDIX 2 MODEL PUBLICATION SCHEME	127

FOREWORD

We all know that being able to access information is a core to any policing service. Our commitment to maintaining public trust and transparency, now more than ever, is under scrutiny.

It lets the people we serve, and our oversight bodies, keep an eye on what we are doing, and helps them make informed decisions about how effective and efficient we are. How we manage our information so that it enables us to discharge our statutory responsibilities under the Freedom of Information Act is one of the services we all provide to keep ourselves honest and transparent.

Sharing information and responding to requests, are the tools we use to convey how we use our resources, fight crime, and keep the public safe.

Of course, there are some things we can't share with the public, because of the nature of our work. But we always try to strike a balance, following the rules and guidance from the Information Commissioner's Office.

High profile mistakes made whilst discharging our FOI duties also remind us that having a professional and assured approach to what we release is also a commitment we make to our own staff too.

This manual is here to help all those who play a role in the FOI process. In particular, it is for your Freedom of Information (FOI) team so they can understand the rules and give practical advice on how to respond to requests. The National Police Freedom of Information and Data Protection Unit is also here to help, giving advice and making sure we're all on the same page to create consistency of service, no matter where our service is delivered. They can even help with training and dealing with complaints. You can reach them at ****S31(1)****

We know that dealing with FOI requests can be tough, but we're committed to being fair and objective. We hope this manual is helpful!

Aimee Smith

National Portfolio Lead for Data
Co-Chair National Data & Analytics Board
Director of Data (Metropolitan Police Service)

INTRODUCTION

PLEASE DESTROY ALL PREVIOUS VERSIONS OF THE MANUAL AND WORK FROM THIS VERSION ONLY

Welcome to the latest version of the NPCC Manual of Guidance for the Freedom of Information Act.

The FOI Manual of Guidance provides the corporate template for processing and managing FOI across the Home Office forces of England, Wales and Northern Ireland, each of which stands alone as an independent public authority.

The manual contains detailed guidance and advice on all aspects of the Freedom of Information Act and its interpretation and implementation. Consideration is also given to identifying the categories of information that the Police Service view as significant and in need of protection.

Looking beyond the FOI request process itself, the manual explains how forces should commit to release information proactively through local publication schemes.

The manual is structured into headings:

Legislation – under this heading the specific section of the Act is presented, along with the exemption type and requirements.

Guidance – the interpretation of the Act and detailed guidance covering good practice in relation to each of the key processes

The purpose of this manual is to provide a template that forces should follow in order to maintain a consistent and coherent approach to the application of the legislation across the Police Service.

Manual Objectives

- To ensure consistency of approach in applying FOI principles, making FOI decisions and enforcing FOI exemptions;
- To act as a user's guide;
- To provide a comprehensive resource for FOI Officers;
- To ensure consistency in publishing information into the public domain via force publication schemes and in response to FOI enquiries; and
- To define those requests that must be referred centrally due to their possible impact on the Police Service as a whole.

POLICE SERVICE REFERRAL CRITERIA

There are certain risks associated with the disclosure of the types of information held by the Police Service. These risks range in severity from the minor upset of a partner agency to the harm of an individual and/or damage to the national infrastructure.

These outcomes can be caused by a wide range of scenarios from criminal, concerted campaign or media use of the legislation to poorly thought out releases or withholding of information. Actually refusing to provide information, even if appropriate, can sometimes be more damaging than releasing it, due to the adverse publicity and complaints it may attract.

Depending on the subject matter and particularly with regards to national requests, it is important that a response from one force does not serve to undermine the response from other forces, or a national approach, set by the NPCC policing lead.

In order to combat these issues, and reduce the risks, a National Police Freedom of Information & Data Protection Unit (NPFDU) was created and ratified by all Chief Constables in the UK. The NPFDU act as a national co-ordination body providing advice and support to forces and stakeholders. This includes centrally coordinating between forces, national portfolio leads and other stakeholders including relevant government bodies, to ensure a national approach.

The NPFDU's remit is to:

- Provide advice, good practice and consistency in response to FOIA requests that meet the referral criteria.
- Co-ordinate strategic development of FOIA throughout the Police Service.
- Maintain and develop relationships with partners, other agencies, regulatory bodies and requestors at a national level.
- Engage and consult with NPCC portfolio leads to determine a national approach.
- Deliver FOIA training and promote good practice appropriate to the needs of the service.
- Proactively monitor potential criminal and misuse of the legislation in order to protect the service.
- Manage intelligence in relation to misuse of the legislation.

THE PROCESS

Forces should analyse all FOIA requests they receive using the referral criteria in this manual. Any request that meets the referral criteria detailed in this manual should be submitted to the NPFDU. Please note updated versions of the referral form and criteria may be submitted to all forces when deemed necessary outside of this manual.

A request being referred must be accompanied by the NPFDU referral form template. Please note that this template must be completed in its entirety for consideration by the NPFDU and incomplete templates will be returned. If information is not available to complete a particular box on the template, please indicate this.

The NPFDU will acknowledge receipt of each referral and the advice will follow as soon as possible, but in any event no later than 10 working days. The NPFDU will, during this time, consult with any relevant stakeholders, including government departments and the Royal Household, to determine the correct course of action. This advice will then be disseminated to forces, providing a consistent national response.

The below list provides current subject areas that require a mandatory referral to the NPFDU. Although some areas are “topical” and may be subject to change, the majority of the listed subjects will remain as mandatory referrals.

There is an additional category for temporary referrals which are added on direction from chief officers/gold groups in relation to specific policing information or incident.

The NPFDU role encompasses providing advice and support to forces at each stage of the FOI process: internal review; ICO appeal; and tribunal stage.

In the first instance issues requiring advice or requests for referral should be sent by e-mail to

****S31(1)****

MANDATORY REFERRALS BY SUBJECT AREA

Mandatory Referrals-By Subject Area	
Subject	Notes
Witness protection/protected persons.	Ultra high risk subject area which must be referred to CRU.
Requests which name and/or relate to information which MAY originate from any of the S23 bodies.	**S23(1)**
Covert operations, use of informants or surveillance activities or tactics.	Ultra high risk subject area which must be referred to CRU.
Counter terrorism (incl Prevent, Pursue, Protect, Prepare) and/or national security material or operations.	Includes SB, CTU, CBRN, port or airport operations, Crowded Spaces and ANPR.
VIP/Royalty Protection.	To include high profile Royal events and visits.
Information received from or which relates to certain partner agencies. *	Includes NPCC, any government department, IOPC, CPS and College of Policing.
Major or complex incidents or investigations or operations. *	Examples such as extremist protests, large scale public disorder, multiple or high profile unexplained deaths, cross border incidents. Will also include national operations and Inquiries.
International Relations	Includes international training, visiting overseas dignitaries & FCO equities where s27 may be engaged.
National Security	Requests requiring s24 will need stakeholder consideration
Notification of ICO complaint, First Tier Tribunal or Upper Tribunal activity	
Requests with potentially significant reputational implications, e.g. the storage of human tissue.	Where national policing leads would welcome the opportunity to comment on high profile matters (if unsure please contact the CRU)
Requests for information held for the purpose of a statutory Inquiry under the Inquiries Act 2005	Examples – UCPI, Manchester Arena, Death of Dawn Sturgess, Grenfell

*If a request is captured by previous NPFDU guidance within the past 12 months, then no referral is required.

Temporary Mandatory Referrals	
Subject	Date added

FREEDOM OF INFORMATION – THE BASICS

THE BASICS

- The Act gives any individual anywhere in the world the right to information held by the Police Service, subject to the application of exemptions.
- The Act gives two related qualified rights – the right to be told whether the information is held and the right to receive the information.
- The right of access applies regardless of the purpose of the application.

PUBLIC AUTHORITY RESPONSIBILITIES

- The duty to confirm or deny whether the information requested exists; and
- The duty to communicate the information.
- The two main instruments through which the release of information is achieved are:
 - **Creating and maintaining a publication scheme** – further detail to be found at Appendix 2. The purpose of this is to make a significant proportion of disclosable information routinely available and accessible without waiting for it to be requested.
 - **Providing a general right of access to all types of ‘recorded’ information held by public authorities**

Under the terms of the Act, public authorities are required to make available requested information (subject to a range of exemptions) to any individual or organisation anywhere in the world.

WHAT IS COVERED?

- Records capable of recovery in any form.
- Information not data or documents.
- Information in any format, no matter how it is recorded.
- Retrospective information: as long as the public authority has the information, it must be considered to fall within the scope of the request.
- All information, no matter how recorded, is subject to the FOIA. This includes written records, typed, handwritten, scribbled notes, e-mails, flip-charts, videos, audio tapes, computer tapes, logs, answer phone messages, tapes of telephone conversations and archived records.

UNDERLYING ALL OF THIS IS THE PRESUMPTION THAT INFORMATION WILL BE RELEASED IN-KEEPING WITH THE SPIRIT OF THE LEGISLATION WHICH EMPHASISES A POSITIVE APPROACH TO DISCLOSURE.

The FOIA gives a general right of access to information to the public. However, the Act makes provision for withholding of information and offers 23 exemptions that may be applied to decline disclosure. For the Police Service, some exemptions are more relevant and applicable than others.

Applying exemptions under the FOIA can be complicated. Detailed guidance is provided in this manual.

ENVIRONMENTAL INFORMATION REGULATIONS

ICO guidance on the Environmental Information Regulations (EIRs) may be located on the relevant ICO's website [guidance page](#)¹

FOI AND ENVIRONMENTAL INFORMATION REGULATIONS (EIR)

There are many similarities between the two regimes and any request for 'environmental Information' must be answered in accordance with the EIRs rather than the FOIA. It is possible that in some cases both regimes will be relevant. In these cases, it is essential to be clear which parts of the information fall under which regime so as to apply the correct exemption or exception, if information has to be withheld.

Requests for information under the EIRs do not need to be made in writing but can include telephone requests on environmental matters (although in practice it is advisable to make a written record of any verbal requests received).

Under FOI there is a requirement to provide a substantive response to any request for information promptly and in any event within 20 working days. There is some scope to extend this timescale when a qualified exemption is being considered and it is necessary to assess the balance of public interest. The EIRs also require requests to be answered within 20 working days but there is provision to extend the response time to 40 working days, but only for complex and voluminous requests.

Appendix 1 covers EIR's in more detail.

¹ [Information Commissioner's Office \(ICO\)](#)

PRE-DECISION MAKING

IS IT A VALID REQUEST?

The first consideration when processing an FOI request is whether or not it is actually valid. If necessary additional information or clarification should be immediately sought from the applicant. For a request to be valid it must meet the requirements of section 8 of the Freedom of Information Act.

LEGISLATION - SECTION 8

****S21(1) Information Reasonably Accessible by Other Means****

Most requests received for information by a force are likely to be FOIA requests and by law must be treated as such. This includes requests made via social networking sites providing they fulfil the section 8 criteria. There is further information in the [Code of Practice²](#) that covers this area.

In terms of names, it is clearly the intention that the real name of the applicant should be provided when an FOI request is submitted. However, forces should not routinely or habitually request ID from applicants unless forces are considering making a request vexatious, in which case the applicants true identify will be a relevant factor.

Where a request is received and the applicant is either anonymous or suspected to be using a pseudonym, there is no lawful requirement to deal with this under FOIA because the criterion defined under section 8 is not met.

However, if there is no harm in disclosing the requested information and there is negligible cost, forces are encouraged to provide the information.

Requests received from companies and charities are also considered valid requests provided the full registered name or a trading name has been supplied. If forces have a reason to check the validity of the company/charity, clarification can be sought from Companies House or the Charity Commission Register.

Campaign groups and clubs are also generally considered valid and should be taken at face value.

² [CoP FOI Code of Practice - Minor Amendments 20180926 .pdf](#)

A valid address can be any address where the applicant can be contacted; postal, email, social media etc. In terms of social media websites, as long as there is a way of responding to the applicant then the requirements under section 8 have been met. For any requests made through the "[What do they Know](#)"³ website, the ICO considers the correspondence address @whatdotheyknow.com, as valid for the purposes of meeting section 8.

If the requested information is not clear and the force asks the applicant for clarification, the request is not considered as valid until the required information is received, and it is at this point that the clock starts.

BUSINESS AS USUAL

To overcome the bureaucratic issues associated with many thousands of pieces of correspondence being processed under FOIA, there is an established option called 'Business as Usual' (BAU). This term has been created to cover certain types of requests which can fall outside of the legislation. It is an informal agreement with the ICO and has no legal basis. Extreme care needs to be taken when taking a request outside of the legislation, as an abuse of BAU could invite an Enforcement Notice from the Information Commissioner's Officer (ICO) or, much more seriously, the withdrawal of the BAU as an option for all public authorities.

To be treated as BAU, a request for information must fit the 'Key Criteria' in that:

- It must not indicate that it is an FOIA request.
- The information will be provided in full.
- The information will be provided within 20 working days.

It is common to receive written requests for information from partner agencies, and other law enforcement bodies, such as the Crown Prosecution Service (CPS), Local Authorities, Independent Officer for Police Conduct (IOPC), Home Office, ****S23(1)**** and other forces.

The provision of information to these bodies is an established key business process, which should not attract the usual FOIA procedure, and should whenever possible be processed as BAU. Care should be taken that just because the requestor is a member of such an organisation, that they are not exercising their private rights under FOIA. If in any doubt then ask the applicant.

However, such requests can only be processed as BAU when the key criteria are met. If the request falls outside of the key criteria, there is still an option to capture it within BAU, provided written confirmation that the requestor does not require it to be processed under FOIA is sought. In the case of any doubt, a formal withdrawal obtained from the applicant will provide an audit trail, protecting the receiving authority.

It is recognised that some information is normally provided for a fee, such as road traffic collision reports. A request for the provision of such data can be dealt with informally if the 'key criteria' are met. Otherwise, the request will need to be processed under the legislation and should attract

³ [WhatDoTheyKnow - Make and browse Freedom of Information \(FOI\) requests](#)

the section 21 exemption, Information reasonably accessible by other means. See also the chapter on the publication scheme.

IS THE INFORMATION HELD?

Under the FOIA any information, documentation or records that are produced internally or held by a public authority, or held by contractors or third parties on behalf of the public authority, are covered by the Act, Section 3(2). This is not limited to “official” documents such as meeting minutes, crime reports and media releases, but will include emails, notes, CCTV recordings, HR records, body worn video etc.

Nor is the information held limited to the information solely created by the public authority, as it will also cover information received into the public authority, for example letters from members of the public, partner agency reports and emails etc. Inaccurate or incomplete records may also fall within the scope of a request, as will draft documents, and all should be considered for disclosure.

When a request is received the public authority will need to consider everything that is captured within the scope of that request, regardless of who generated the information originally. This also includes information held off-site or information held by a contractor working on behalf of the public authority.

If decision makers experience some resistance to accessing information held by third party contractors, section 3(2) of the FOIA states that information held by a public authority includes “information held by another person on behalf of an authority”, this includes material that has never physically been held by the public authority. Forces should consider the contract between the force and the third party as a good starting point in establishing how much of the information held by the third party is for their own purpose and how much is held on behalf of the force. Although this may not be recorded explicitly within the contract, it should contain indicators confirming the information the third party has to provide. Further information can be found within [ICO guidance](#)⁴

Deciding if information is considered “held” for FOI purposes can be difficult to navigate and should be determined on the facts of each case, as demonstrated in a [recent DN](#)⁵ (FS50855937) which states, for information to be considered “held” there has to be “*an appropriate connection between the information and the authority*” and that each part of a request should be considered on its own merit.

Information held by staff associations will not be covered by the Act, even though the information may be held on police servers or premises. This is provided that the information is for the sole use of those associations and is not used for a policing purpose, in which case it is not considered “held” by the authority under the FOIA.

However, if the information is used or accessed by the police force to execute its functions as an

⁴ [Information you hold for the purposes of FOIA | ICO](#)

⁵ [FOIA-EIR decision notice template](#)

organisation, then it would be deemed as being held by the Police Service and needs to be considered for disclosure under the FOIA. This also applies to information provided to forces by suppliers and contractors and to information they hold or have collated on behalf of the forces.

IS THE INFORMATION IN THE PUBLIC DOMAIN?

Part of your pre-decision making should be considering whether the requested information is already in the public domain as this will affect your decision making process.

For information to be considered in the public domain, it must be reasonably accessible to a member of the public at the time of the request. This can include information available for a fee.

The information should be locatable using a simple internet search and must not require any specialist knowledge to find it.

Forces should consider the provenance of the information and only direct the applicant to a credible source of information, for example government and partner agency websites. There is a great deal of information available in the public domain, including statistical data on recorded crime, Chief Officer salaries and expenses, budget information and press releases, to name a few.

Information may enter the public domain for a while, but this does not mean that it stays there indefinitely, for example a response to a previous FOI request, or information revealed in open court. This is called a “window of opportunity” and consideration should be given to whether a member of the public could realistically access the information at the time the request is received.

Should there be some related information in the public domain this does not automatically fall in favour of disclosure of the additional information. Consideration should be given to any harm caused by creating a mosaic effect of combining this information with information already in the public domain.

IDENTIFYING HARM

The main reason for not complying with section 1(1) of the Act is that some kind of prejudice would occur. This is labelled by the Police Service as ‘harm’ and although no such definition exists within the Act, this is the beginning of the process that will determine whether an exemption could apply.

It is the responsibility of the decision-maker in the first instance to collect evidence of all the potential harm that might result from disclosure of the information, and subsequently to determine the likelihood of the harm occurring if it is not certain or probable.

Although harm need not be substantial, the ICO expects it to be more than trivial. It must be real and not perceived. The degree of harm is not specified, so strictly any level of harm or damage might be argued. However, forces should bear in mind that the less significant the harm is shown to be, the higher the likelihood that the public interest test will require disclosure.

It is unlikely that decision-makers will be experts in the relevant business area of the information requested so it is imperative that, where possible, stakeholders are identified and, where appropriate consulted, including third parties that may be outside the organisation. Doing so will ensure that the evidence of harm and public interest factors are properly gathered.

SECTION 9 FEES

LEGISLATION – SECTION 9

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Public authorities must comply with a request for information, provided the information can be located, retrieved and extracted within the appropriate limit, or if exemptions apply. However, a public authority can charge for the cost of complying with the request and the amount is determined by section 9 of the Act.

Section 9 provides regulation for public authorities to be able to charge for the cost of expenses incurred, for example photocopying or postage, when the cost of complying with the request itself does not exceed the appropriate cost limit.

For example, a request costs the public authority £300 to locate, retrieve and extract the information, which is below the £450 appropriate limit, so the request must be dealt with. There are additional costs to the public authority for photocopying 200 sheets of paper at 10p per sheet, totalling £20.

The public authority can issue a fees notice for £20 in accordance with section 9.

They cannot charge the £300 for the time taken to locate, retrieve and extract the information.

GUIDANCE

A fees notice should be issued to the applicant stating the amount of the fee and how to pay it. This must be done within the 20 working days from receipt of the request, however, this time is included within the time for compliance (section 10).

If the fee is not paid within 3 months the public authority is no longer obliged to respond to the request.

Further information can be found on the [ICO website](#)⁶.

⁶ [Fees that may be charged when the cost of compliance exceeds the appropriate limit | ICO](#)



SECTION 10
TIME FOR COMPLIANCE WITH REQUEST

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 10 provides the response time frames that a public authority must adhere to. The time limit in which forces have to respond to requests is very clearly defined in the legislation and ICO guidance. Requests must be answered as soon as practicably possible, and in any case within 20 working days. It is important to remember that day '1' will be the day after receipt.

There is a possibility that the deadline can be legally extended for public interest considerations but only where a valid qualified exemption is engaged. This option should not be taken unless the force is considering public interest issues.

There is no provision to support occasions where forces cannot comply because of issues such as poor records management, lack of resources or internal failings due to members of the force not participating effectively in the request process.

ICO guidance clearly articulates that consultation and research with stakeholders is not a valid reason for non-compliance in respect of exceeding the time limit on requests.

The 20 working day time limit starts the day after receipt of the request and this would be considered as the day the request is physically or electronically delivered. If you have sought clarification from the requester then the date of receipt would be the date that the clarification is received.

Where clarification has been sought from the applicant and no response has been received, the section 45 Code of Practice confirms the authority may close the request after two months. This should be clear in communications with the applicant.

If section 8 of the Act is not complied with, then the 'clock' will not have started as a valid request does not yet exist.

If a request is received into an unmanned email address which has an 'out of office' directing to an alternative address, the request has not been 'received' and the onus falls back on the applicant to re-direct. If an 'out of office' is on with no alternative, then the request was received on the date it arrived in the original mailbox.

PIT EXTENSION

Where a qualified exemption is being applied, the public authority may extend the deadline for consideration of public interest factors for a time which is reasonable in the circumstances. The FOIA does not define the word 'reasonable', but it is the ICO view that a public authority should take no more than an additional 20 working days to assess the public interest considerations. In cases where the public interest considerations are exceptionally complex, it may be reasonable to take longer but, this should only be in exceptional circumstances

The applicant should be kept regularly informed of progress and where the initial 20 working days is going to be exceeded, forces must still serve a 'refusal notice' under section 17 of the FOIA within 20 working days of a request, even in those cases where it is relying on a qualified exemption and has not yet completed the public interest test

That notice must state the exemption(s) being relied on and, if not apparent, why. The notice must include an estimate of the time by which this decision will be made. If the final decision is to withhold the information requested, a second notice must then be issued providing the reasons for the decision on the public interest. No further notice is required if the final decision is to disclose the information.

In some situations, a qualified exemption may apply to the duty to confirm or deny and, due to the need to consider the balance of the public interest, it may not be appropriate to confirm or deny whether the information is held within the 20 working day deadline. If time for complying needs to be extended in relation to the duty to confirm or deny, the letter to the applicant must be very carefully drafted to ensure that no indication is given as to whether or not the information requested is held.

Also remember that if no exemptions apply to some of the information requested, it should be provided within the 20 days as usual. The time deadline for the provision of this information cannot be extended. It would be good practice to provide this information together with the extension notice.

It is recommended that a PIT extension response should include:

'The FOI Act obliges us to respond to requests promptly and in any case no later than 20 working days after receiving your request. We must consider firstly whether we can comply with s1(1)(a) of the Act, which is our duty to confirm whether or not the information requested is held and secondly we must comply with s1(1)(b), which is the provision of such information. However, when a qualified exemption applies either to the confirmation or denial or the information provision and the public interest test is engaged, the Act allows the time for response to be longer than 20 working days, if the balance of such public interest is undetermined.

In this case we have not yet reached a decision on where the balance of the public interest lies in respect of either of the above obligations. We estimate that it will take an additional [xx] days to take a decision on where this balance lies. Therefore, we plan to let you have a response by [date]. If it appears that it will take longer than this to reach a conclusion, you will be kept informed.

The specific exemption(s) which apply in relation to your request is/are: [include both qualified and absolute indicating which is which and include a brief explanation of why it/they apply unless it is not apparent or unless you are not required to do so by virtue of s17(4)].

Insert usual complaint information.'



SECTION 11 MEANS OF COMMUNICATING INFORMATION

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 11 is only relevant when information is being disclosed by the public authority, and allows the applicant to express a preference for how this information is communicated to them, referred to as the “means of communication”.

Section 11 places a duty on the authority to comply with the preference specified by the applicant at the time the request is made, it is not relevant after you have started to deal with the request or if you have already provided the information. It allows for a choice of 3 ways to communicate the information, of which the applicant may choose more than 1 option:

- A copy of the information
- An opportunity to inspect the information
- A digest or summary of the information

Forces may receive requests for the information to be provided in a particular electronic format such as Word; PDF; Excel etc. which should be adhered to whenever possible and practical to do so. However, if forces choose to provide the information in a re-usable format (pivot tables) they must ensure that any “hidden” information is removed so as not to disclose data unintentionally. Best practise would be to extract the information into a new Word document.

The ICO provided additional guidance to public authorities following several major data breaches, focussing on the challenges and risks of inadvertent disclosure of personal information when providing information in a spreadsheet. It asked public authorities to ensure they **no longer disclosed original source data to online platforms**. This means ensuring any spreadsheets received by practitioners from business areas are either converted into other open reusable formats such as Comma-Separated Value files (CSV), or request an alternative address to respond to. Further information can be found online:

[Information Commissioner’s Office - Advisory note to public authorities | ICO⁷](#)

Further information regarding release of data in an excel spreadsheets can be found under section 11A & 11B.

Under section 11(1)(b) the applicant has the right to request to inspect a record containing the information they wish to see, and this means the whole record and not just the information extracted from it.

The duty of the public authority is to comply with the applicants request if it is ‘reasonably practicable’ and for the majority of forces requests this will not be the case, however, the force will have an obligation to provide the information to the applicant through other means.

Should the applicant request information as a summary, there is no requirement under the Act to create information, however, the ICO would consider forces have conformed with

⁷ [Information Commissioner’s Office - Advisory note to public authorities | ICO](#)

s11(1)(c) if a summary can be produced by extracting parts of the information requested.

This does not mean the requester can use s11(1)(c) to obtain a 'non-exempt' summary of the exempt information, so if exemptions apply to the information in part or full, s11(1)(c) does not apply.

This section is not covering requests for a pre-existing summary, for example the executive summary from a management meeting.

In determining if it is considered 'reasonably practicable' to provide the information in a specified, preferred format, public authorities can consider the following;

- The cost of complying. This is in relation to the work involved, and does not count towards the s12 cost limit.
- How the document is held – would copying a very old and fragile document damage it?
- Resources that are available to the public authority.
- Security issues or physical restrictions that would prevent members of the public from entering premises to inspect records.

Further guidance can be found on the [ICO website](#)⁸. This provision also covers Datasets which is covered next.

⁸ [Means of communicating information \(section 11\) | ICO](#)

**SECTION 11A & 11B
DATASETS**

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

SECTION 11B POWER TO CHARGE FEES IN RELATION TO RELEASE OF DATASETS FOR RE-USE

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

The dataset provisions were added to the FOIA by [The Protection of Freedoms Act 2012⁹](#) and is concerned with how the information is released, rather than the content itself, and about the re-use of those datasets. The sections with the FOIA that have provisions for datasets are 11, 11A, 11b, and 19 (publication scheme). The provision relates solely to the FOIA and not to the EIR.

The ICO confirms a dataset is a collection of factual information in electronic form to do with the services and functions of the authority that is neither the product of analysis or interpretation, nor an official statistic and has not been materially altered. This does not only apply to numerical data and could capture other factual information, e.g. Lists of addresses.

The information must be held by the public authority as a dataset and be provided as part of a FOI response or under a publication scheme, in a way that allows them to be re-used. The applicant has the right to request the information is released in an electronic format and if so the public authority must provide it in a re-useable form, as far as is reasonably practicable. The same considerations as set out at section 11 apply to whether it is 'reasonably practicable' to do so, for example, the time and cost of conversion, any technical difficulties and resources can be taken into account.

A request for a dataset should initially be treated in the same way as a request for any information under the Act; so the first consideration should be whether it can be

⁹ [Protection of Freedoms Act 2012](#)

located, retrieved and extracted within cost as per section 12(1) and whether any exemptions are relevant. Ahead of applying section 11 public authorities should first consider if any information held as part of the dataset would be exempt from disclosure, in particular they should consider whether any personal data may be disclosed.

Redacting information under an exemption from a dataset, does not change the definition of the dataset.

The request does not have to state the information provided should be in a re-usable format as this is implied for all requests received electronically, provided the information is held in a dataset. For requests asking for hard copies of information, there is no duty placed on the public authority to provide a re-useable format. If the information provided is as a result of data being extracted from various sources and a new list or table of data is compiled, possibly with additional calculations, then this is not considered a dataset as the new table or spreadsheet is not data that has been obtained or recoded to provide the authority with information in connection with its services or functions, and the material has been altered.

A re-usable format is one where the information is available in a machine-readable form (meaning software applications can easily identify, recognize and extract specific data); use open standards (meaning the public can use it without any restrictions) and based on open standards (details specifications for requirements of software interoperability). The ICO considers CSV format capable of re-use under this definition.

If a dataset is provided as part of a response it would be considered best practice to publish this as part of your publication scheme. If the public authority concludes it would not be reasonably practicable to provide the dataset in a re-usable format, then the authority must still provide the dataset in another format and address within the FOI response the reasons it was not possible.

It is best practice that, so long as there are no good reasons for it not to be provided, that datasets will be accompanied by sufficient metadata and contextual information about how and why the dataset was compiled or created in order that applicants may fully understand the dataset they are dealing with

Public authorities must also ensure that they own the copyright and database rights in a dataset before licensing it for re-use and should release datasets with accompanying details of licence conditions that apply to the re-use of the dataset or otherwise any limitation on re-use by virtue of third party intellectual property rights.

Further information can be found on the [ICO guidance¹⁰](#).

DISCLOSING INFORMATION SAFELY

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

¹⁰ [Datasets \(sections 11, 19 & 45\) | ICO](#)

Best practise for FOI units is to extract any information provided by business areas into new documents such as Word. Forces should not use the original source spreadsheet.

Practitioners should avoid disclosing data in excel spreadsheets or pivot tables, and instead export the data into CSV or other reusable formats, where only visible text is exported. The ICO guidance advises against using spreadsheets with hundreds or thousands of rows. Practitioners should ensure disclosure of information is in the most appropriate and secure format, which may involves copying the information into a different file format. For example, for charts, exporting the document into PDF format will remove the underlying data.

Should FOI units choose to provide the information in Excel spreadsheets, extreme caution should be taken to ensure responses do not include 'hidden data'. In other words the 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' to view the full data. Other examples include hiding entire workbooks, or using password protection, neither are considered best practice. The metadata may also contain the name of the document creator. A workbook containing many open 'sheets' can appear to have closed those sheets when they are no longer visible on the screen, however, they remain within the workbook and accessed via the 3 small dots at the foot of the workbook.

To be certain there is no hidden data, practitioners can export the spreadsheet to CSV, which will export all the information from the current tab/workbook, including hidden rows or columns. Once identified, only relevant data can then be imported into a new spreadsheet to make sure there is no hidden data in the file.

Pivot tables within excel, and other software, can also contain hidden data. A pivot table can be used to summarise a large set of data housed within other worksheets, which although not visible within the response, and may in fact 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 they were created, the underlying data may still be retrievable via double-clicking on the chart.

It is recommended that all officers and staff:

- Do not upload original source spreadsheets to online platforms used to respond to FOI requests. If it is not possible to provide the same information in a more secure format such as CSV, request an alternative address for correspondence.
- Review existing processes to ensure all FOI responses that contain Excel spreadsheets are reviewed before release to ensure no 'hidden data' is contained within the files. The ICO have produced a checklist for public authorities to use - [disclosure-checklist¹¹](#)
- For any FOI request relating to personal data ensure there is a final double-check of any disclosure by another member of the team
- Ensure that all staff dealing with FOI responses fully understand their obligations and [ICO guidance¹²](#) in respect of removing personal data from information requests and datasets.

¹¹ [disclosure-checklist-v1_0.docx](#)

¹² [How to disclose information safely](#)

ICO Checklist and sign off for public authorities to use for the safe disclosure of information from Excel

Information request reference	[Reference]	
Consideration of excel data	Checked by	Secondary check by
Are you sure you know where all the data is?	[staff name]	[staff name]
Have hidden columns been deleted if not part of the request?	[staff name]	[staff name]
Have hidden rows been deleted if not part of the request?	[staff name]	[staff name]
Have hidden work sheets been deleted if not part of the request?	[staff name]	[staff name]
Has any linked data been removed from pivot tables if not part of the request?	[staff name]	[staff name]
Has any linked data been removed from charts if not part of the request?	[staff name]	[staff name]
Have any links to external files from formula, or hyperlinks, been deleted if not part of the request?	[staff name]	[staff name]
Has any personal information been removed if not part of the request or not disclosable (including from any 'comments' or 'notes')?	[staff name]	[staff name]
Has any special category personal information been removed if not part of the request or not disclosable (including from any 'comments' or 'notes')?	[staff name]	[staff name]
Has any meta data been removed if not part of the request?	[staff name]	[staff name]
Is the file size larger than you might expect for the volume of data being disclosed?	[staff name]	[staff name]
Conversion of data	Converted by	Checked by
Has the file been converted to CSV (Comma-Separated Value) format?	[staff name]	[staff name]
Publication of data	Considered by	Checked by
Have you considered alternative ways to disclose, other than an online platform?	[staff name]	[staff name]
Management sign off	Signed off by	Date
The above staff members have been trained in how to disclose information safely before preparing this response	[managers name]	[date]

SECTION 12 REQUESTS WHERE THE COST OF COMPLIANCE EXCEEDS THE APPROPRIATE LIMIT

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 12 of the FOIA 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 Fees Regulations state that this cost limit is £450 in the case of the Police Service and £600 for Central Government.

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** (section 12(2))

THE APPROPRIATE LIMIT

There are two distinct areas in relation to fees contained within the legislation. The first area is relevant to the initial processing of a request when an authority, when estimating the time taken, can take into account the following four items:

- Determining if the information is held;
- Locating the information;
- Retrieving the information; and
- Extracting the information to be disclosed from the other information.

The time spent identifying information to be exempted and the time dedicated to the process of redaction cannot be included in the fees estimate. This could, however, be considered under section 14 as a burdensome request.

Example

A request is received for any external feedback on the force's new IT project.

The information is contained somewhere within a mixture of electronic files and hard copy letters and correspondence contained within 10 crates. The total number of documents is in excess of 10,000 and to read through each of those documents to determine those relevant to the request is likely to exceed the 18 hours.

A similar request is received for **all** information held relating to the force's new IT project. The same information is identified as being relevant to the request. There is now no requirement to filter out irrelevant documents as all the information is captured by the request. The fact that these documents now need to be read in order for a disclosure decision to be made is not something that can be included within the fees estimate

CALCULATING COSTS

An authority can take into account the costs attributable to the time that persons (both the authority's staff and external contractors) are expected to spend on these activities. Such costs are calculated at £25 per hour per person for all authorities regardless of the actual cost or rate of pay, which means that the limit will be exceeded if these activities exceed 24 hours for central government, legislative bodies and H.M Armed Forces, and 18 hours for all other authorities, including the Police Service.

NB. The figures of £450 and £600 relate only to the appropriate limit; they do not relate to the fees that may be charged.

ESTIMATE

Section 12 makes it clear that a public authority does not have to make a precise calculation of the costs of complying with a request. Only an estimate is required. However, the estimate must be **reasonable**.

Good practice when refusing a request on cost is to provide a breakdown of how those costs have been estimated.

Where a force refuses a request because the appropriate limit has been exceeded, it should advise and assist the applicant to refine their request in order to bring it under the cost threshold.

This may include indicating if it would be possible to provide any information within cost, and to narrow down the request appropriately.

SUBSECTIONS

Section 12 has several subsections that are to be adhered to when issuing a section 12 refusal notice. Examples of when they are used within the Police Services are:

12(1) –this subsections confirms the information is held, however, to locate, and retrieve it would exceed costs.

12(2) – If to confirm the information is held, would in itself exceed costs, then using this subsection would act as a “neither confirm nor deny” provision.

When applying section 12, it should be made clear within your response letter what your position is, ie whether it would exceed the appropriate limit to determine whether you hold the information, or if you have established that you hold the information, but it would exceed the limit to gather it.

12(4) – this subsection covers aggregation of 2 or more requests from either one person or by a number of persons acting in concert. The request must be for the same or similar information and received by the public authority within any period of 60 working days. This period takes into account the responsibility to respond to requests within 20 working days, however, the aggregation period can run 60 working days ‘backwards’ from the date of any request under consideration.

Note: Multiple questions on one request constitute separate requests for information.

SECTION 13 FEES FOR DISCLOSURE WHERE COST OF COMPLIANCE EXCEEDS APPROPRIATE LIMIT

LEGISLATION SECTION 13

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 13 states that a fee may be charged for requests that exceed the appropriate limit. This is referred to as a marginal cost and can include finding, sorting, editing and redacting information, communicating the information and staff time.

Section 13 allows public authorities to choose to answer a request which exceeds the appropriate limit and make an appropriate charge.

If a public authority is offering to provide the information for a fee then it should issue a fees notice. Although there is no statutory requirement to do this, as there is no obligation on the authority to comply with a request when section 12 applies, it allows the applicant the option of receiving information upon payment of a fee.

As a matter of good practice a public authority should also aim to provide a fees notice as soon as possible and at least within the 20 working day period for responding to the request.

THE CURRENT NPCC POSITION IS NOT TO ACCEPT PAYMENT AND APPLY SECTION 12 WHERE APPROPRIATE.

SECTION 14 VEXATIOUS REQUESTS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Under section 14(1) of the Act, 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.

Section 14(1) may be used in a variety of circumstances where a request, or its impact on a force, cannot be justified. In most cases a refusal notice must still be issued within 20 working days.

The term 'vexatious' is not defined in the legislation. In [ICO vs Devon County Council & Dransfield¹³](#) the Upper Tribunal defined the purpose of Section 14 as '...must be to protect the resources (in the broadest sense of that word) of the public authority from being squandered on disproportionate use of FOIA...!'.

Although the term vexatious is not defined in the Act and the Tribunal in the above case took the view that the question of whether a request is vexatious depends on the circumstances surrounding that request. The Tribunal concluded that 'vexatious' could be defined as the '...manifestly unjustified, inappropriate or improper used a formal procedure.'

Forces should not regard section 14(1) as something which is only to be applied in the most extreme circumstances, or as a last resort. The ICO encourages authorities to consider its use in any case where they believe the request is disproportionate or unjustified.

It is important to note that it is the request - not the requester - that is made vexatious. A public authority cannot refuse a request on the grounds that the requester themselves are vexatious.

However the application of section 14 requires the gathering of evidence and like all decisions made under FOI can later be subject to external scrutiny. It is imperative that its application is proportionate and relevant to the prevailing circumstances and a full record is kept.

The four broad themes considered by the Dransfield tribunal can be categorised as:

¹³ <https://administrativeappeals.decisions.tribunals.gov.uk/judgmentfiles/j3680/%5B2015%5D%20AACR%2034ws.rtf>

- the burden (on the public authority and its staff);
- the motive (of the requester);
- the value or serious purpose (of the request); and
- any harassment or distress (of and to staff).

The key question to ask therefore is whether the request is likely to cause a disproportionate unjustified level of disruption, irritation or distress. This will need to be balanced against the level of public interest in the issues.

IDENTIFYING AND DEALING WITH A VEXATIOUS REQUEST

The ICO suggests that there are some typical key features of a vexatious request:

Abusive or aggressive language

The applicant's tone goes beyond the level of criticism that an authority should reasonably expect to receive.

Burden on the authority

The effort to meet the request will be so grossly oppressive in terms of the strain on time and resources that the authority cannot reasonably be expected to comply.

Personal grudges

Targeting a particular employee against whom they have some personal enmity.

Unreasonable persistence

Attempting to reopen an issue which has already been addressed or otherwise subject to some form of independent scrutiny

Unfounded accusations

Makes completely unsubstantiated accusations

Intransigence

Requester rejects attempts to assist and advise out of hand and shows no willingness to engage.

Frequent or Overlapping requests

Frequent correspondence about the same issue or sends in new requests before the authority has had an opportunity to address their earlier enquiries.

Deliberate intention to cause annoyance

Requester has explicitly stated that it is their intention to cause disruption.

Scattergun approach

Request appears to be part of a completely random approach, lacks any clear focus, or seems to have been solely designed for the purpose of 'fishing' for information.

Disproportionate effort

The matter being pursued is relatively trivial and the authority would have to expend a disproportionate amount of resources in order to meet the request.

No obvious intent to obtain information

Requester is abusing their rights by using the Act as a means to vent their anger

Futile and Frivolous requests

The issue individually affects the requester and has already been independently investigated or is inane or extremely trivial.

BURDENSOME

A public authority cannot apply section 12 to the cost and effort involved in redacting information or considering exemptions. However, it can consider applying section 14, if it can evidence that the amount of time required to review and prepare the information for disclosure would be burdensome to the authority.

There is no set time or cost for this within the Act, however, the ICO will weigh up the public interest in disclosure of the information, when reviewing cases, and where the public interest in the disclosure is high, it is not considered unreasonable for the time spent on preparing information for disclosure to be well over the 18 hours allocated under section 12.

The context and history in which a request is made will often be a major factor in determining whether the request is vexatious, and the public authority will need to consider the wider circumstances surrounding the request before making a decision as to whether section 14(1) applies.

In practice this means taking into account factors such as:

Other requests made by the requester to that public authority (whether complied with or refused);

The number and subject matter of those requests;

Any other previous dealings between the authority and the requester;

And, assessing whether these weaken or support the argument that the request is vexatious.

There is no set time or cost for this within the Act, however, the ICO will weigh up the public interest in disclosure of the information, when reviewing cases, and where the public interest in the disclosure is high, it is not considered unreasonable for the time spent on preparing information for disclosure to be well over the 18 hours allocated under section 12.

REPEATED REQUESTS

There is also a separate provision under section 14(2) when a request can be refused if it is repeated. To engage this section, the following must be established:

- It was made by the same person as a previous request
- It is identical or substantially similar to the previous request, and
- A reasonable interval has not elapsed since the previous request

A public authority is not required to comply with the request for information if they have previously provided the same requestor with the information via a previous FOI request, or they have confirmed the information is not held in response to a previous FOI request.

The 'reasonable interval' is not defined within the Act but it is suggested that 60 working days may be a useful benchmark. However this is subject to the prevailing circumstances such as the information changing on a regular basis, or a newer version becoming available shortly after the request was dealt with

REFUSING THE REQUEST

When a vexatious or repeated request has been received, a refusal notice must be issued within 20 working days. The refusal notice should state that either section 14(1) or section 14(2) is engaged, together with an explanation as to why. Details must also be provided in respect of the force's internal review procedure and the right to appeal to the ICO.

However, section 17(6) states a refusal notice need not be issued if the same applicant has already received a refusal notice for a previous vexatious or repeated request **and** it would be unreasonable to issue another one

Requests cannot be refused under this section if they are submitted by different persons, unless there is a belief that they are part of a campaign designed to cause disruption or annoyance, in which case section 14(1) may apply. It may be simpler to aggregate them for the purposes of cost under section 12, if there is a belief that requesters are acting together and compliance would exceed the cost limit.

SECTION 16 DUTY TO PROVIDE ADVICE AND ASSISTANCE

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

- The Police Service has a duty to provide advice and assistance to applicants making FOI requests.
- Whilst there is no requirement to acknowledge a request under the Act, the Police Service will acknowledge all requests received. The acknowledgement should include the date the request was received and contact details for the FOI Team.
- Where necessary, the applicant should be contacted to clarify the request as soon as possible.
- Procedures for dealing with FOI requests should be published under the force publication scheme.
- Under the FOIA, **all** members of staff within an organisation are obliged to provide assistance to any person requesting information, this could be front counter staff, and may start before your request is actually received, i.e. the applicant may call requesting assistance in the wording of a request.
- Where an applicant is unable to make a request in writing (for instance due to illiteracy, disability or illness), a note of the request can be made on behalf of the applicant and sent to them for confirmation.
- If advice and assistance has been provided and the force is still unable to identify and locate the requested information, the force is not expected to seek further clarification.
- Where further clarification has been sought and the applicant has not responded, the force may close off the request after 60 working days if no further clarification is received.

It is good practice and highly recommended that the applicant is contacted, verbally if possible, to try and assist in identifying the exact information required from the authority. In the case of media organisations, it is recommended that this contact is purely about the request and where the media organisation is asking specific questions about the police force, they should be directed to the Media Services Department.

Section 16(2) confirms that if a public authority adheres to the Section 45 Code Of Practice guidance on advising and assisting applicants, then it will have complied with its duty under

under section 16 of the Act.

If a request is refused (on cost or exemptions) and the public authority chooses to provide “harmless” information to the applicant, this should not be done under the banner of section 16. This information is provided outside of the Act, and therefore, section 16 should not be quoted in your response.

TRANSFER OF REQUESTS

Guidance for transferring request can be found in the Section 45 Code of Practice.

Requests may be completely transferred where the force holds none of the information requested, or partially transferred where the force holds some of the information requested. In both cases the applicant must be informed as soon as possible that no/partial information is held.

The public authority receiving the request may transfer it to the new public authority, but only with the consent of the applicant.

A request should not be transferred without first confirming with the second force or public authority that the information is held.

Alternatively the force may suggest that the applicant re-applies to the authority it believes holds the information. The force should provide the applicant with contact details for the relevant authority

CONSULTATION WITH THIRD PARTIES

When a third party may be affected by disclosure, the Police Service will 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 Act and the individual circumstances of the request.

There may be contractual obligations that require discussion or with a view to gaining a better understanding of the information sensitivities being requested.

Where the interests of more than one third party are affected and they have a representative organisation, consultation with the representative organisation, or a representative sample of third parties if there is no representative organisation, is sufficient.

If a third party does not respond to consultation, the force has a duty to disclose information under the Act within the time limits.

In all cases, it is the receiving force/authority that determines whether information should be disclosed. A refusal to consent to disclosure by a third party does not, in itself, mean that information should be withheld.

SECTION 17
REFUSING A REQUEST

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

When refusing either all or part of a request for the following reasons, then a refusal notice must be issued in order to comply with section 17 of the Act:

- The request is deemed vexatious or repeated;
- The cost of compliance exceeds the prescribed limit; or
- The information requested falls under one of the exemptions listed in part II of the Act

There are three occasions when a refusal notice is not required. These are:

- If it appears that a request is vexatious or repeated and there has already been a refusal notice issued to the applicant in relation to a recent similar request stating that the request is vexatious or repeated and it would be unreasonable to do so again.
- If no information is held in relation to the request, although this must still be confirmed in writing and within the 20 day deadline.
- Where section 8 of the Act has not been complied with.

A refusal **must** state that the information is being refused, specify the exemption(s) in question and (if it is not otherwise apparent) state why the exemption applies (Please also refer to the NCND chapter).

This means in practice that the section and subsection of an exemption must be used and its title, which type of exemption it is (qualified, absolute etc.) and an explanation as to what it means and if it is not obvious, why it applies.

If NCND is **not** being applied and qualified and/or prejudice-based exemptions are engaged, the section 17 notice will also need to contain the evidence of harm, the public interest test and the balance test. Plain English should be used wherever possible and the duty to advise and assist the applicant should always be borne in mind.

A refusal notice should contain full details of the authority's complaints procedure and particulars of the rights conferred by section 50 (complaint to the ICO) must be included in all responses.

A summary of the subsections uses are:

- 17(1) Exemption applied
- 17(2) PIT Extension
- 17(3) Exemption applied following PIT extension
- 17(4) NCND
- 17(5) section 12 or section 14
- 17(6) Previously vexatious or repeated
- 17(7) Complains or appeals process

SECTION 19 PUBLICATION SCHEMES

INTRODUCTION

Section 19 of the Act places a duty on public authorities to adopt, implement, operate and maintain a publication scheme. The publication scheme is an integral part of compliance with the Freedom of Information Act and serves as the ongoing indicator that public authorities are committed to openness and transparency.

A well-managed, up-to-date publication scheme will ensure that information is proactively published in accordance with the spirit and intentions of the Act to make information available to the public.

It is important to note that the proactive publishing of information is an organisational responsibility and not solely a matter for FOI Officers. There are wider organisational benefits than those related solely to compliance with the Act. Aside from improved transparency and openness, forces can:

- Manage the content, format and timescales of the publication of information;
- Make wider use of information it already produces for other purposes such as for Police Authority or Home Office use;
- Divert requests for information from the bureaucracy of the FOI process; and
- Enable FOI Officers, when responding to FOI requests, to make greater use of section 21 and section 22.

LEGISLATION

Any publication schemes created before 1st January 2009 are now out of date. The ICO has produced a model publication scheme that can be adopted, without modification by any public authority and without further approval, to be used by all public authorities (see appendix 4).

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications.
- To specify the information held by the authority that falls within the classifications.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within the scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made available proactively.

- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information.

The scheme includes:

- Classes of information and a general definition of those classes;
- The method by which information will be made available; and
- Circumstances where charges may be made.

The listed information is the **minimum standard** to which forces are required to adhere.

Further [guidance¹⁴](#) is available on the ICO website along with a model of the publication scheme.

GUIDANCE

Forces should have a link to 'Freedom of Information' displayed on their force web-site. The link will direct the public to the Publication Scheme, which will list the following documents:

[The ICO Model Publication Scheme 2009¹⁵](#)

[The Police Sector Definitions Document¹⁶](#)

Guide to Published Information - a detailed section on this document appears below.

Forces are required to produce a Guide to Information, which details the information it will routinely make available, how the information can be accessed and any applicable fees. This information, along with the model scheme should be available on the authority's website. Each piece of information must be located on the website or accessible via other means to the general public. This can include hard copy information that may be sent out on request. Any information not suitable to be published on a website should still be included in the Guide to Information along with contact details allowing the public to make a request to see it.

There is no requirement to make a paper copy of the entire contents of the published information available in libraries or other public areas. However, any public contact points, e.g. front desk at police stations, reception staff, switchboard staff, should have sufficient understanding of how to assist the public if they make a request for information, including checking whether the information is already published or available..

¹⁴ [ICO's publication scheme compliance | ICO](#)

¹⁵ [model-publication-scheme.pdf](#)

¹⁶ [definition_document_for_police_forces.pdf](#)

All staff with a role in handling enquiries from the public must be made aware of the Guide and how to access it.

The published information can be held on a page relevant to that subject matter, on another website or in paper or disc format held by the owning department. However, forces may choose to operate the traditional method of grouping the published information together. If information is not grouped together, the Guide should contain links.

The model scheme introduces the concept of 'routinely making information available'. It is not necessary to have all the information in full on the force web-site; this can often be impractical due to the size of documents. The Guide will state how the information can be accessed: i.e. a link to the relevant page on the force web-site, a link to another web-site, a contact number for the public to use to ask for a copy of the information to be sent to them, arrangements for coming into force to view the information.

As well as listing what information is available, your Guide will explain how often the information is updated, whether previous data is still available and for how long, and when data will be archived.

The starting point for ensuring that the required information is made available is the Police Sector Definitions Document which provides guidance for police forces on the generic classes of information listed in the model publication scheme.

The ICO expects authorities to regard the publication document as a 'minimum requirement' and to provide all the information listed unless it can be legitimately excluded.

Information can be legitimately excluded where:

- It is not held;
- It is exempt from disclosure by virtue of an exemption in the FOI Act; or
- The information is not readily available, e.g. the information has been archived in accordance with records management policy; the information is held in an obsolete format and would require specialist techniques to retrieve it

MONITORING AND REVIEW

The model scheme includes a requirement to review the information published under the scheme, so forces should have a process in place to do this.

Forces can approach this in one of two ways:

- The FOI Officer is responsible for adding and updating the information as it becomes available.
- The department owning the information is responsible for adding and updating the information, with the FOI Officer conducting a review at least annually to ensure the publication scheme is being maintained.

In either option, a review should be carried out in conjunction with departments to ensure that best use is being made of the publication scheme and to assess whether new information is being produced that should be made public.

FEES AND CHARGES

The expectation of both the ICO and NPCC is that information will be provided free of charge. A charge can be made in exceptional circumstances and this should be made clear in the Guide to Published Information. Charges can be made for disbursements, e.g. photocopying, postage, or where the authority is legally authorised to charge.

It is NPCC policy that a charge should be made only in exceptional circumstances and where the charge can be fully justified. Information published on the force website will not attract a fee (including disbursements) if it is requested in hard copy format. Information that is 'made available' can attract a fee for disbursements where the document is large or where the person requests that it is made available in a particular format, e.g. copied to disk or CD. Forces should refer to the disbursements section of the Fees Regulations section 9.

COMPLAINTS PROCEDURE

The information on your force website should include details of how to make a complaint or provide feedback about how the force is operating its publication scheme, and forces should adopt a process to deal with such complaints.

The ICO has powers to enforce compliance of a publication scheme, or failure to publish required information, regardless of whether a complaint has been received.

FOI PERFORMANCE DATA

As all police forces are separate public authority and have over 100 full time equivalent (FTE) employees, details of your FOI performance handling should also be published. This is part 8.5 of the section 45 code of practice¹⁷.

The ICO have provided a template that forces can use (How to report on your performance on handling requests for information under FOIA 2000 | ICO)¹⁸ and the information can be published on forces websites.

Alternatively, the CRU collate the 'key data' monthly statistics which are published on the NPCC Website¹⁹, so forces can publish a link to the website to satisfy this criteria.

¹⁷ [Freedom of Information Code of Practice - GOV.UK](#)

¹⁸ [How to report on your performance on handling requests for information under FOIA 2000 | ICO](#)

¹⁹ [FOI and Subject Access Request](#)

NCND

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

THIS IS A MANDATORY REFERRAL TO THE NPFDU WHEN USING S23(5) & S24(2)

GUIDANCE

GENERAL

The Act refers to the first duty as 'the duty to confirm or deny', although the second duty – to provide the information - is the area most applicants will be concerned about and generates the bulk of decision maker's work.

However, when simply confirming information is held will in itself disclose exempt and therefore harmful information, practitioners should ensure that they carefully consider how they comply with both section 1(1)(a) and section 1(1)(b) independently and chronologically.

Both have equal weight and if qualified exemptions apply they will require slightly different public interest tests. A justified application of the need to NCND in terms of section 1(1)(a) removes the legal obligation to then comply with section 1(1)(b). Put simply, if an absolute exemption or the public interest, in terms of a qualified exemption, upholds the right to NCND there is no need to further consider the request in terms of disclosure.

It is equally important to consider a NCND response, when information is held and when it is not.

THE NCND PRINCIPLE

In addition to obvious situations where confirmation or denial is harmful, for example confirming you hold 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'.

One of the biggest risks is when failure to abide by the principle either causes problems with future requests or handicaps other forces or bodies who wish to apply the NCND, but are now restricted because the principle has been compromised somewhere else.

Example: A force is asked for the information that they hold on any surveillance operations in relation to particular premises. Any information held is likely to fall within the section 30 exemption, as it is held by that authority for the purposes of a criminal investigation. But, unless it is already in the public domain, it is unlikely that you would want to confirm the existence of such an operation.

However, simply refusing to provide the requestor with the information would not go far enough to protect the integrity of this, or any other surveillance operation. If the police force were to confirm or deny that they have the information then that would, in itself indicate whether or not the police have had an interest in the premises concerned.

To disclose even that amount of information could be prejudicial to any operations or investigations that are taking place or may take place in the future. Hence the necessity to NCND the response under section 30(3) of the Act.

It is irrelevant whether any such operation were even taking place.

If NCND were only applied when information was held this would disclose that which you are trying to protect. Therefore it is important to consider the “NCND Principle” and apply it in all cases where it is reasonable to do so, not only when the information is held.

PARTIAL NCND

There can be circumstances where a partial NCND is engaged; a force may confirm that some information is held (this may be supplied or exempted) although to confirm that this represents all the information in the possession of the authority would in itself be harmful. Authorities may then add to their response that they neither confirm nor deny (under the respective exemption) that any other information is held. This more frequently occurs with the use of exemptions section 23 and section 24 considered below.

NCND and its relationship with section 23 and section 24.

One of the most common reasons to apply NCND is when there is a need to protect the involvement of exempt bodies in relation to police activity. This is where the ‘NCND Principle’ often needs to be considered.

Example: A force receives a request for information relating to a publicly avowed child abuse investigation. The decision maker confirms that information is held under section 1(1)(a) and applies section 30 and section 40 to remove the need to disclose the information under section 1(1)(b).

****S23(1) Information supplied by, or concerning certain security bodies****

As you can see this is a complex concept and it is when there is no section 23 information in the first place that practitioners often need to think of possible future requests and alternative scenarios to ensure the principle is maintained.

As part of the package of support and in order to minimise the risk to the Police Service and our partner agencies the NPFDU consult with many stakeholders including government departments and agencies, to support decision making in relation to section 23 and section 24 material. It is therefore vital that any application of these exemptions are referred.

There is considerable potential overlap between the information covered by section 23 and section 24. Whereas the first applies to certain bodies, the latter relates more to the type of activities that they undertake. Therefore the information requested may attract both exemptions. However, when used substantively they are mutually exclusive and cannot be applied to the same information. This changes when applying the NCND, when it is then technically permitted to apply both exemptions, provided that if the information existed it would be either section 23 or section 24.

What is not permissible is the use of a substantive section 23(1) or section 24(1), in terms of section 1(1)(b) and then a partial NCND using either or both section 23(5) or section 24(2). If this situation arises there are other options, which is to apply the substantive 'in the alternative' or simply rely on the NCND only.

[ICO Guidance²⁰](#) provides further information.

Example: **S23(1) Information supplied by, or concerning certain security bodies**

The latter basically means that you apply both exemptions but do not reveal which actual one is properly being relied upon. In our fictional case the use of either option will be dictated by what is already in the public domain and the best protective strategy as agreed with partner agencies via NSLG.

However, please note that the application of section 23 and 24 in the alternative is being considered at Upper Tier Tribunal (UTT), therefore, we ask that forces refer all cases requiring consideration of these sections to the NPFDU where up to date guidance will be provided.

²⁰ [How sections 23 and 24 interact | ICO](#)

RESPONDING TO THE APPLICANT

When a public authority refuses either to disclose requested information or confirm or deny that any information is held, it must under section 17(1) of the Act, issue a refusal notice stating the fact of refusal, the exemption used and why the exemption applies. A public authority should be clear in its refusal notice that where the public interest test applies, it has applied it in relation to each duty individually. That said, section 17(4) states that a public authority is not obliged to make a statement as to the reasons why NCND is engaged IF the statement itself would involve the disclosure of information which in itself would be exempt. It is the view of the Information Commissioner that whenever possible public authorities should provide an explanation on why the NCND principles are engaged, though if this will compromise the NCND stance then a standard section 17(4) statement can be provided.

SECTION 17(4) REFUSAL

An example of a section 17(4) refusal is shown below:

The [force] neither confirms nor denies that it holds any of the information requested. To give a statement of the reasons why neither confirming nor denying is appropriate in this case would itself involve the disclosure of exempt information, therefore under section 17(4), no explanation can be given. To the extent that section [add section] applies, the [force] has determined that in all the circumstances of the case the public interest in maintaining the exclusion of the duty to neither confirm nor deny outweighs the public interest in confirming whether or not information is held.

This whole field is complex and requires considerable experience both in selection of appropriate exemptions and the framing of a response which will need to consider the issues surrounding section 17(1) and section 17(4) responses. Guidance can be obtained from the NPFDU and as previously stated consultation with relevant partner agencies is essential.

The core skills required in order to successfully and effectively apply NCND is the need to think outside of the request, outside of the your own force boundaries and also be able to work in the abstract environment of considering all the possible types of information that could be held in any type of circumstances. It is often more effective to consider the NCND principle before ascertaining what information, if any, you do hold.

INTERNAL REVIEW PROCESS

GUIDANCE

Part VI of the section 45 Code of Practice places a duty on public authorities to implement a complaints process to ensure that applicants are able to request an internal review if they are not content with an authority's response. This provides a first review stage for applicants. The Code of Practice states a public authority is not obliged to accept a request for an internal review if it is received after the fortieth working day following the original response being issued.

If a complaint is received from a dissatisfied applicant, written acknowledgement of receipt must be provided to the applicant with an indication of when a response may be expected.

The Act does not stipulate a time limit for reviews but the section 45 Code of Practice states a response should be provided within 20 working days of receipt. This is extendable in exceptional circumstances by another 20 working days.

It is important to be aware that the internal review stage is an opportunity to consider a case completely afresh. Compliance with the legislation is an important component of the process but all relevant considerations should be revisited and appropriately documented.

Internal reviews should not be overly bureaucratic. They are intended to be a fair and impartial means of reviewing the original request process and best practice dictates this should be completed by someone other than the original decision maker.

The original process should have produced a record of how the original decision was made and this record will provide important information to those conducting the internal review.

The applicant must be fully informed, in writing, of the outcome of the internal review. In all cases, there is a requirement to notify the applicant of the result of the internal review. If revised exemptions or public interest test are being relied upon, a new section 17 refusal notice must be issued.

Whatever the result of the review, the applicant must be made 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.

GENERAL CONSIDERATIONS

- The review should be undertaken by someone different from, and preferably senior to, the original decision-maker.
- Those forces, whose organisational and process structures make this difficult, should focus on the consideration that the main need is to be able to demonstrate the independence of the reviewer from the influence of the initial process and its decision-maker.:

- The reviewer should preferably be trained in and have a good understanding of Freedom of Information issues or be able to directly seek advice from such a person.
- If the nominated reviewer or reviewers have no Freedom of Information experience then they should identify a suitably qualified person to assist with the review, particularly if the main issues relate to legal compliance. The advisor should preferably be someone who had no involvement in the original request.
- It should, where possible, be a one stage procedure and as prompt, thorough, clear and simple as is practical.
- If at all possible, this should apply even when the matter relates to complex matters or significant strategic issues and the review is carried out by a panel.

The following checklist may assist forces in processing internal reviews.

FREEDOM OF INFORMATION ACT AND EIR REVIEW CHECKLIST

PROCEDURE	Were timescales adhered to?	
	Was the requestor kept informed?	
	If any of the requested information was held by another authority, was the request, or part of the request, appropriately transferred?	
RELEVANT INFORMATION	Was all the requested information held located and recovered correctly?	
	If there was any difficulty, what action has or can be taken to address this matter? (E.g. has appropriate discussion taken place with the information owner?)	
	Were issues regarding inaccurate or misleading information appropriately conveyed to the requestor?	
ORIGINAL DECISION	Did the response 'no information held' accurately reflect the circumstances?	
	Was the request correctly defined as 'repeated' or 'vexatious'?	
	Were the grounds for any refusal appropriate and correctly explained to the requestor?	
	Have circumstances changed since the original decision was made?	
	Would further disclosure now be possible, beneficial or desirable?	
	Were appropriate exemptions cited?	
	Was suitable evidence provided to demonstrate they were engaged?	
	Were any prejudice and public interest considerations correctly addressed?	
	Were submissions made by the information owners regarding the appropriateness of information disclosure suitably considered?	
	Was any other local or national advice regarding the information considered in the original response?	
	Did the original response letter meet the requirements under s17 of the Act?	
REVIEW DECISION	Does the review decision support the original decision?	
	Is the release of additional information appropriate?	
	Were any shortcomings in original process identified?	

<p>REVIEW CONCLUSION The Complainant</p>	<p>Have you informed the complainant within 20 working days of the result of your review? (Note – the result communication should clearly set out the decisions and provide the rationale for those decisions in the same manner as an initial Freedom of Information response. Even where the original decision is supported the reasoning and explanations should be reiterated to some degree).</p>	
	<p>Have you disclosed any additional information or clearly articulated the steps to be taken to provide access to the information (e.g. visit to a particular site)?</p>	
	<p>Have you apologised for any identified inadequacies in the original process?</p>	
	<p>Have you provided contact details for the Information Commissioner’s appeal process and the necessary instructions on how to initiate an appeal?</p>	
<p>Original Decision-Maker</p>	<p>Has appropriate feedback been provided to the original decision-maker (including the result of the review and suggestions for the future handling of similar requests)?</p>	
	<p>Have you identified any additional training needs?</p>	
<p>The Organisation</p>	<p>Have you informed the relevant information owners, providing comment and advice where their opinion on any release does not reflect the decision of the review?</p>	
	<p>Have you checked that all those with an interest in the result of the review are informed?</p>	
	<p>Have you identified any need to change business processes, provide training or raise awareness within the organisation?</p>	

THE PUBLIC INTEREST TEST

OVERVIEW

Qualified exemptions contained within the Freedom of Information Act are subject to the application of the public interest test. Even if such 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. If the balancing test is equal, the default option should be to disclose.

The 'public interest', is not however, what the public may find interesting, there must be some tangible benefit to the community in such a disclosure. Ultimately it must be something that serves the interests of the public. It is a requirement to identify all the factors which serve these interests and also those which do not, only then can a decision be made.

Under the FOIA, an authority must apply the public interest separately to each relevant exemption. This is to ensure that a force does not then rely on an exemption which the PIT has overcome. The public interest must not be used on its own to refuse to disclose information; it must only be used in conjunction with an exemption.

The exemptions subject to the application of the public interest test are listed in the table below.

SECTION	EXEMPTION
Section 22	Information intended for future publication
Section 24	National security
Section 26	Defence
Section 27	International relations
Section 28	Relations within the UK
Section 29	The economy
Section 30	Investigations and proceedings conducted by the public authority
Section 31	Law enforcement
Section 33	Audit functions
Section 35	Formulation of government policy
Section 36	Disclosure prejudicing the effective conduct of public affairs
Section 37	Communication with Her Majesty and the awarding of honours
Section 38	Health & safety
Section 39	Environmental information
Section 42	Legal professional privilege
Section 40	Personal Information (on rare occasions)
Section 43	Commercial interests

GUIDANCE**THE DUTY TO CONFIRM OR DENY AND THE PIT**

Under Section 1(1)(a), an authority is under a duty to confirm or deny whether it holds information requested. This duty does not arise where the public interest in maintaining the exclusion of the duty to confirm or deny outweighs the public interest in disclosing.

To this end most exemptions also contain a subsection which allows a 'neither confirm nor deny response', if appropriate.

Practitioners often make the mistake of only considering the public interest in relation to disclosing the information, (section 1(1)(b)). It is important to also be aware of the requirements to consider the PIT in relation to section 1(1)(a), if there is harm in confirming or denying that information is held and a qualified exemption is being relied upon, a PIT must be completed.

The difficulty is in grasping the point that the debate now will be purely based on the issues with confirming or not that the information actually exists, rather than disclosing it.

Reference should be made to the separate chapter in this manual on neither confirm nor deny, but the below fictional case study may assist in understanding the differences.

Example

Force's A and B are asked for the technical details of a particular piece of covert equipment. Harm is identified that engages section 31(3) Law enforcement, as confirming or not whether the information is held will disclose the forces tactical capability. Section 31 is a qualified exemption, so the decision-maker has to first consider the PIT in relation to confirming whether the information is even held.

In Force A the PIT issues identified are the detrimental impact to the public of that equipment becoming compromised versus their right to know of its usage and that funds for fighting crime are appropriately spent. On balance, as the procurement processes in place and independent financial auditing serve the needs of the public in ensuring that funds are spent appropriately, it is decided that the former is the most persuasive argument and an NCND stance by virtue of section 31(3) is the response provided.

In Force B, the PIT issues are virtually identical except that also favouring confirmation or denial is the fact that the force took part in a 'fly-on-the-wall' programme which showed the equipment being used. On balance it is found that the public interest is better served by confirming information is held and section 31(3) is overcome.

Force B then have to move on to consider the PIT in relation to section 31(1) as disclosure of the technical information requested will enable criminals to put in place counter measures. Now, the issues are the effects on the public of crime being more difficult to detect versus them being better informed, enabling more accurate debate and accountability. It is decided that the balance lies with the former and the force confirms information is held, but refuses to disclose it by virtue of section 31(1).

CONDUCTING THE PUBLIC INTEREST TEST

A thorough, effective test will largely depend on the decision-maker's research, coupled with the ability to make out reasoned arguments. It should be objective, but it can become subjective if the individual either does not possess the relevant skills or is unduly influenced by external influences and/or their own views and prejudices.

The public interest test should be applied in a manner that is in-keeping with the spirit of the Act. That is to say there is an assumption that public authorities will provide information requested unless an exemption applies and the public interest favours retention of the information over disclosure. The burden of proof lies with the decision-maker to establish whether there are sufficient grounds to justify an exemption.

The starting point for conducting the test becomes the collation of all the relevant factors. It is unlikely that any one individual can provide all of this information and it should be obtained from a variety of sources. If not approached in this manner there is a risk that the views of the person providing the factors actually dictate the end result, or their own lack of knowledge is detrimental to the process.

The below fictional case study may help demonstrate this point:

Example

Forces A and B receive identical requests for statistical data on rape in a small policing team area. The FOI Officer in Force A asks the force Performance Department, who produce the statistics, for any harm in disclosure and if so what the PIT considerations might be. The response is that they can see no harm.

The information is disclosed, this raises public awareness in the area, resulting in a local news item and an offender ceasing their activities due to the publicity. This compromises an ongoing covert operation.

In Force B, the FOI Officer asks for any Harm and PIT considerations from the Performance Department, the policing teams Sergeant and the DCI responsible for the force's rape strategy. From the Sergeant they learn of several local community issues, and the DCI tells them about an ongoing covert operation and the problems a disclosure will cause. The FOI officer works through the information provided and finds there is sufficient harm to engage s31(1), the PIT looks at the issues of the detriment to the public in a potential rapist escaping justice versus the need for the community to be aware of current issues. The balance falls in favour of non-disclosure, and a complex refusal notice is issued. They brief the SIO on the covert operation and the force media department. The local media are engaged and work with the police to not highlight the refusal as it appears on the force disclosure log. The offender is brought to justice a short time later and then together with the usual media releases, the FOI officer puts the statistics into the public domain.

We have established that the role of the decision-maker is to identify all the relevant issues and incorporate those into a decision making framework. The full process is outlined in this manual and the following is just the PIT phase.

1. Identify **all** of the exemptions that are engaged with the disclosure of the information.
2. Filter those exemptions to identify which ones are qualified and which are absolute. It is suggested that if many exemptions are engaged there is little benefit in using all of them and the most appropriate ones should be used. There can be a temptation to rely only on absolute ones, as there is no PIT, but you should only do so if they are firmly engaged, and actually cover all of the information requested.
3. For every qualified exemption there is a need to identify and outline the positives and negatives in disclosure in relation to each exemption. When considering public interest factors in favour of maintaining the exemption, a public authority should only consider the particular interest which the exemption seeks to protect, for example the prevention of crime. In contrast, the public interest factors in favour of disclosure are not restricted in this way, and can include the general public interests in the promotion of transparency, accountability, public understanding and involvement in the democratic process.
4. If the PIT obviously favours disclosure then that exemption should then be disregarded.
5. The remaining exemptions then need to be looked at as a whole, to see if the balance of the PIT favours disclosure. Only now can a decision be made.

The following table of some of the exemptions more commonly used by the police service and the issues likely to be relevant may assist in your research. It is not an exhaustive list, and the weight of each point will vary from case to case. It also does not take into account the harm that may have been identified even though this will always be relevant to the public interest.

To be valid factors in favour of non-disclosure, there must be a clear relationship between the factors, the information and the exemption and this must be articulated. Factors favouring disclosure can be more generic and wider in nature.

A recent tribunal ruled that PIT arguments can be aggregated, confirming that the FOIA permits the public interest recognised in two or more different provisions in Part II (exemptions) to be assessed in combination or aggregated in determining whether the public interest in maintaining the exemption of the information from disclosure outweighs the public interest in disclosure [The Department for Business and Trade v The Information Commissioner & Anor - Find case law - The National Archives](#)²¹

²¹ [The Department for Business and Trade v The Information Commissioner & Anor - Find Case Law - The National Archives](#)

EXEMPTION	NON-DISCLOSURE	DISCLOSURE
Section 22	<ul style="list-style-type: none"> • The publication date is imminent. • There may be a duty to present the information to another body or person first eg. Police Authority, Coroner, staff association, IPCC. • It would disrupt a press strategy designed to elicit information from or to inform the public. • The publication is being prepared at some expense to the force and the spending of additional public funds would be wasteful. 	<ul style="list-style-type: none"> • Information is only in draft form and is likely to change significantly when published. • The publication will not provide everything that was requested. • The date for publication is in the distant future. • The information relates to mistakes made by the force.
Section 24	<ul style="list-style-type: none"> • It is 'reasonably necessary' to apply the exemption. • The risk of harm to the public would increase. • Ongoing or future operations to protect the security or infrastructure of the UK would be compromised. • Security measures would be rendered less effective. 	<ul style="list-style-type: none"> • The information simply relates to national security and disclosure would not actually harm it. • The information relates to mistakes made by the force. • Better informed public can take steps to protect themselves. • Use of public funds. • The information relates to mistakes made by the force.
Section 30	<ul style="list-style-type: none"> • An investigation would be prejudiced. • The right to a fair trial would be undermined. • The force's future law enforcement capabilities would be affected. • Maintaining a confidential source. • Hinder the prevention or detection of crime. • Undermine the partnership approach to investigations. 	<ul style="list-style-type: none"> • The investigation is closed and any proceedings have been completed. • Satisfaction that the investigation was conducted properly. • The prosecution collapsed because of procedural failure or mis-management. • Use of public funds. • The investigation is high profile or national.

Section 31	<ul style="list-style-type: none"> • Law enforcement tactics would be compromised. • A fear of crime will be realised. • Individuals are placed at risk. • Hinder the prevention or detection of crime. • Impact on police resources. • More crime could be committed. • Undermine the partnership approach to law enforcement. 	<ul style="list-style-type: none"> • Better awareness may reduce crime or lead to more information from the public. • The information relates to mistakes made by the force. • The public would be able to take steps to protect themselves. • Some information is already in the public domain.
Section 38	<ul style="list-style-type: none"> • The risks to individuals are significant and evidenced. • Loss of confidence in the public authority to protect the wellbeing of the community. 	<ul style="list-style-type: none"> • The evidence provided does not reveal a 'significant risk' to the physical or mental health or the safety of an individual. • Better informed public awareness and debate. • Use of public funds. • The information relates to mistakes made by the force.
Section 43	<ul style="list-style-type: none"> • Damage would occur to an ongoing tender process. • Civil action from third party will take place. 	<ul style="list-style-type: none"> • Better understanding of how public funds are spent. • The information is historic. • Funds have been misspent. • Better understand the decision-making process.

CONSIDERATIONS THAT ARE INVALID

In addition, there are a number of criteria that may not be considered as part of the public interest test or may be applied only in limited circumstances:

EMBARRASSMENT	Potential embarrassment to the force, Police Service or an individual officer on release of information is not a valid public interest consideration in favour of non-disclosure.
HIGH PUBLIC OFFICE	Where the subject of the information, the giver or the recipient of the information holds high office, this is not in itself sufficient to weigh against disclosure. An assessment of the consequences of the disclosure of the particular issue is required.
POLICY DEVELOPMENT	Even where information relates to policy development, this does not establish a public interest consideration favouring non-disclosure. Even if policy is under review, it still may be in the public interest to release.
CANDOUR AND FRANKNESS	Claims that disclosure would prejudice the supply of frank and candid information in the future can only be considered where there is a very particular factual basis to support this view. The possibility of future publicity through disclosure may deter immediate release and should provide an incentive to improve the quality of the information/record prior to disclosure.
DISCLOSURE OF CONFUSING OR MISLEADING INFORMATION	In most cases, the force would have a means of avoiding such a prejudicial effect by releasing new or revised information to rectify any inaccuracies or clarify the situation. If a certain course of action has not been considered and should have been, this is not enough to withhold.
INFORMATION/RECORDS HELD DO NOT FAIRLY REFLECT THE REASONS FOR A DECISION	Where this occurs, the force would have the opportunity to provide additional information that accurately explains the reason for the decision.
DRAFT DOCUMENTS	There may be benefits of public access to draft material, to further the accountability and public planning process. Draft documents may therefore be disclosed. Disclosure of this kind allows members of the public to examine the process by which a decision has been reached, thus serving the public interest.
GOVERNMENT SECURITY CLASSIFICATIONS POLICY	The marking of material under the GSC will not, in itself, be valid grounds for withholding information. GSC indicates how a document should be transported, handled and stored. The content of the material should be examined and the relevant exemptions applied only after discussion with the data owner and other relevant parties. Time elapsed since the document was marked under GSC may also be a factor in any decision to release or withhold.

BALANCE TEST

After establishing all the facts for and against disclosure, and filtering out those exemptions which are obviously overcome, a decision then has to be made on what are the most persuasive arguments. This is probably one of the most challenging areas for a decision-maker, especially if it appears that others within the organisation have already made up their minds, without proper consideration of these factors. Force policies and procedures should support and empower FOI staff to make proper decisions, based on the evidence that they have before them. This requires high levels of skill and judgement and is not purely an administrative function. It is imperative that they are appropriately trained and have access to not only all the information requested but also the background and history of everything relevant to the case.

When applying the PIT, the factors favouring disclosure and non-disclosure should always be recorded, this will form the basis of any future audit trail and help justify disclosure or non-disclosure in the event of challenges or appeals to the decision. It will also form the basis for any refusal notice. If released, it can be kept in a less formal format.

FOI EXEMPTIONS

SECTION	EXEMPTION	TYPE	TYPE
Section 21	Information reasonably accessible by other means	Absolute	Class-based
Section 22	Information intended for future publication	Qualified	Class-based
Section 23	Information supplied by, or relating to, bodies dealing with security matters	Absolute	Class-based
Section 24	National security	Qualified	Class based
Section 26	Defence	Qualified	Prejudice-based
Section 27(1) Section 27(2)	International relations International relations	Qualified Qualified	Prejudice-based Class-based
Section 28	Relations within the UK	Qualified	Prejudice-based
Section 29	The economy	Qualified	Prejudice-based
Section 30	Investigations and proceedings conducted by the public authority	Qualified	Class-based
Section 31	Law enforcement	Qualified	Prejudice-based
Section 32	Court records	Absolute	Class-based
Section 33	Audit functions	Qualified	Prejudice-based
Section 34	Parliamentary privilege	Absolute	Class-based
Section 35	Formulation of government policy	Qualified	Class-based
Section 36	Prejudice to the effective conduct of public affairs	Qualified	Prejudice-based
Section 37	Communication with Her Majesty etc and honours	Qualified	Class-based
Section 38	Health & safety	Qualified	Prejudice-based
Section 39	Environmental information	Qualified	Class-based
Section 40	Personal information	Absolute (in part)	Class-based
Section 41	Information provided in confidence	Absolute	Class-based
Section 42	Legal professional privilege	Qualified	Class-based
Section 43(1) Section 43(2)	Commercial interests	Qualified Qualified	Class-based Prejudice-based
Section 44	Prohibitions on disclosure	Absolute	Class-based

SECTION 21 INFORMATION REASONABLY ACCESSIBLE BY OTHER MEANS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

The purpose of this exemption is to ensure that there is no right of access to information via FOIA if it is available to the applicant by another route. The public authority must still comply with its section 1(1)(a) obligations and confirm or deny if the information is held by them.

If not all of the information is in the public domain, then section 21 will only be relevant to that part of the request. The applicant's individual circumstances can be taken into account when considering application of this exemption and part of your assessment should be whether or not the requested information is reasonably accessible to the applicant who has requested it.

When using this exemption, the applicant must be provided with details of where the information may be obtained from. The provision of information under the FOIA is generally free of charge (apart from what's allowable in the Fees Regulations). However, it is permissible to cite this exemption when the information is normally provided for a fee. For example, road traffic accident/collision reports.

A public authority **must clearly indicate** on its publication scheme if it is making a charge for the supply of information. It may be appropriate to include on the publication scheme a list of

Documents and other information that is available for a fee.

Charges for information may be made where:

- Information is already provided for a fee under a statutory scheme; and
- The information is already published as part of the authority's publication scheme and a charge has already been indicated for the class of information in question.

This exemption may be applied if the information requested is publicly available on a website (not just the force's own website) or in the publication of another individual, organisation or publisher.

To apply this exemption, information must be physically and geographically accessible to the applicant. If it is available in one location only and there is a requirement to source the information in person, this may not be considered 'reasonably' accessible.

The publication scheme must specify the format in which information is published. Information provided in electronic format should be offered as a hard copy alternative for those applicants without reasonable access to the Internet.

Where a public authority has a legal obligation to publish certain types of information, this too should be considered reasonably accessible, even though it may not appear on, or be described in, the publication scheme. This applies if the information requested is available by virtue of the legal obligations of another public authority to publish.

The exception is information that is available only on inspection, by visiting a specific location for example. In this case, the information is not considered to be reasonably accessible even though the authority has a legal obligation to publish it (unless it falls within a class of information that is included on the authority's publication scheme).

Information that is normally made available in inspection is not 'reasonably accessible' if:

- The applicant lives a considerable distance away;
- The applicant has mobility problems; or
- There are other factors that may influence an applicant's ability to view the information.

In these cases, the authority may consider providing a hard copy of the information – though this does not mean it is obliged to every time.

The authority is under no obligation to translate information that is published in response to a request into other languages. It may, however, be reasonable for the authority to translate the original request and then consider translation on a case-by-case basis.

Public authorities should be aware of their obligations under other legislation such as the Equalities Act 2010 and the Welsh Language Act 1993. For example where an applicant has a disability or may require the information requested in an alternative form – such as in Braille or an audio-tape – the onus is on the authority to consider providing it in the format requested.

Public authorities may also have their own internal policies that commit them to delivering a certain level of service for members of the non-English speaking community. It is important that members of staff responsible for dealing with FOI requests are aware of existing policies regarding access to information for those with physical disabilities or for non-English speakers.

When a special case is put to the authority for information published, where disability or other difficulties result in problems in accessing the information (such as a lack of internet access), then it will be left to the individual force to decide on how best to provide the applicant with the information requested.

When considering the application of this exemption, FOI officers can take into account the identity and circumstances of the applicant. For example, section 21 may be used where the applicant is an employee of the organisation and is able to access information on the force's Intranet.

Section 21 can only be relied upon under CPIA (Criminal Procedure and Investigations Act 1996) if the information has already been provided under CPIA and not on speculation that it may be provided under CPIA. In circumstances where it is known that a request is being made for unused material subject to the CPIA, then the applicant should be reminded that an application under that Act must be made in addition to or instead of the FOIA request.

SECTION 22 INFORMATION INTENDED FOR FUTURE PUBLICATION

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 22 may be engaged if, at the time of the request, the public authority has the intention to publish the specific information requested. Without this intention, section 22 may not be used and authorities may not take the decision to publish the information **after** the request for information is received.

To rely on section 22 forces must, at the date of the request, hold the requested information with the intention of publishing it

This exemption is concerned with the **timing** of the release of information. It is not concerned with the suitability of the **content** for release. Having said that, the content being considered for publication must include all the specific information requested by the applicant.

The actual publication date is not required for section 22 to be engaged. However, the Act states that the publication date must be 'reasonable'. Where the date for publication has still to be determined, section 22(1)(c) may only be cited where it is reasonable to postpone publication until an unspecified date.

Even though there is no requirement to have a settled date in mind for publication, there must be a settled intention to publish. It's not enough to be intending, at a future date, to consider whether to publish.

It is not necessary for the publication to be planned by the public authority receiving the request.

Section 22 also covers information that another authority or person (individual or organisation) intends to publish. One public authority, for example, may have been given a draft or document for consultation that another intends to publish.

Where a request for information is directed at information that falls within a class defined in the authority's publication scheme, it may be assumed that the information is intended for publication, even if it has not already been published. Thus, the decision becomes one relating to timing rather than disclosing or withholding the information. The authority must consider whether it is in the public interest to release information earlier than originally planned.

In relation to the harm that might result from the disclosure, this is only relevant if it results from the early disclosure ahead of the scheduled release date. The harm is not in the information itself as there was an intention to publish it in the future anyway.

It is generally the case that the sooner the intended date of publication, the stronger the case for applying the exemption.

Even if the information is in a draft form and may be amended or omitted prior to the final version being agreed, this exemption still applies. Whilst the words may differ from draft to final document, the information imparted probably will not. Where the information exists in draft or rough form only or if it forms a part of a larger body of work or information, it may be more difficult to apply section 22.

SECTION 22A RESEARCH

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 22A was added to the Act in October 2014 with the intention to specifically cover information relating to ongoing research. It applies to information obtained in the course of or derived from a programme of research where the research is on-going and there is a plan to publish a report of the outcome.

Provided the research is still ongoing the exemption will apply, provided there is an intention to publish a report of the outcome at a future date. Any such report may or may not include the specific information requested without affecting the application of the exemption. There does not need to be an intention to publish the exact information requested.

The public interest test is similar to that of section 22, in that it is greatly around the timing of the publication and the ICO is in support of researchers completing the programme and finalising their findings before it is subject to public scrutiny.



SECTION 23
INFORMATION SUPPLIED BY, OR CONCERNING CERTAIN SECURITY
BODIES

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

THIS IS A MANDATORY REFERRAL TO THE NPFDU

GUIDANCE

Any request received by forces that has the potential to include information relating to a security body, must be referred to the NPFDU for consultation with relevant stakeholders. The term 'relates to' is interpreted widely and includes any information concerning or linked to the activities of a security body. If it is more likely than not that the information relates to a security body, then the exemption is engaged (balance of probabilities). However, as referenced in Upper Tier Tribunal [MPS & ICO V's Rosenbaum²²](#), this is not unlimited, and a judgement will need to be made on whether this connection is too remote to be applied.

Although the purpose of section 23 is to preserve the operational secrecy necessary for s23 bodies to function, practitioners should also consider whether the retrieved information can be disaggregated from the section 23 material and provided in a redacted format. Section 23 can be used for information originating from a security body that is provided by a third party. In this way, the exemption can protect intelligence as it is disseminated through different channels. Sometimes though, the relevant security body do not want it known that the information has originated from them, therefore section 23(5) is required instead.

Section 23(5) provides an exemption from the duty to confirm whether information is held where such a confirmation or denial would itself disclose information relating to a security body. Sometimes a force may not hold any information on a specific individual/investigation/tactic for example but to state 'no information held' would show that the security bodies are not interested in that person/investigation/tactic, (which in itself, is information relating to a security body). If however, a few months later the same request is submitted but now the security bodies are interested in that person/investigation/tactic and information is held, exempting the information or applying a NCND will indicate that sensitive information on that individual/ investigation/tactic is now held, relating to the security bodies. By applying an NCND 23(5) in the first place will protect information relating to the security bodies that is or is not held, now and in the future.

This consistent application of the NCND 23(5) in these types of situations will protect when and where the security bodies (**S23(1)**) have, or have not been involved in certain investigations or do or do not use certain types of police tactics. However, this consistent use of 23(5) is restricted to circumstances where there is a risk of establishing a pattern that if deviated from, would signal a change in the activities of the security bodies.

Although section 23 is an absolute exemption and there is therefore no requirement to articulate the harm or PIT for the exemption, occasionally the public authority will need to explain its grounds for applying section 23(5) to the Commissioner, especially when it is used in

²² [IN THE UPPER TRIBUNAL](#)

a consistent manner such as above. In exceptional cases, the Commissioner may need to know if the information is held and may require access to it in order to understand its nature and provenance.

'In the territory of national security' – this is a phrase used by the ICO and means that there has to be a realistic possibility that a security body would be involved in the issue that the request relates to and that the public authority would hold that information.

Section 23 cannot be used as a blanket exemption and each piece of information captured by a request should be considered separately (referred to as disaggregation), as demonstrated in the Upper Tier tribunal case of [Cordery and Ahmed v Information Commissioner, Attorney-General and Cabinet Office](#)²³.

Examples of when section 23 would be applied:

Material relating to Special Branch or Counter Terrorism units, because they work closely with security bodies and routinely share information and intelligence with them. This was confirmed in the ICO DN FS50788439:

The Commissioner accepted that there may be instances where SB information would not relate to a s23 body, but these would be few and far between.

Other examples of when section 23 could be applied would be for information on police tactics such as phone tapping or covert methodology, when security bodies may work closely with the Police to gain intelligence.

Section 23(1) is subject to the public interest test where it is applied to information in a historical record held by the National Archives or the Public Records Office Northern Ireland. An historical record was one that was over 30 years old but this has been amended to 20 years by the Constitutional Reform and Governance Act 2010, Part 6, s46(2) which will be phased over a 10 year period, decreasing until it reaches 20 years in 2023.

Section 23(1) and 24(1) are mutually exclusive which means that section 24(1) can only be applied to information that does not fall within section 23(1) and therefore cannot be applied to the same information. However, it can be cited 'in the alternative'. This is explained further under the NCND section and in full within the ICO guidance titled, ['How sections 23 and 24 interact'](#)²⁴.

²³ [High Court Judgment Template](#)

²⁴ [How sections 23 and 24 interact | ICO](#)

SECTION 24 NATIONAL SECURITY

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

THIS IS A MANDATORY REFERRAL TO THE NPFDU

GUIDANCE

Sections 23 and 24 are often very closely linked.

The section 23 exemption is applicable to information received from or related to a number of bodies specifically listed in the Act (see section 23) and is applicable to information which is necessary to safeguard national security.

Section 24(1) can only be applied to information that does not fall within section 23(1). This means it cannot be applied to the same information but it can be cited 'in the alternative'. This means that although only one of the two exemptions can actually be engaged, the Commissioner has stated that a public authority may refer to both exemptions in its refusal notice, so as not to reveal whether a S23 security body is involved.

In certain circumstances, it will be necessary to use the two exemptions together. In other circumstances the two exemptions are mutually exclusive and cannot be used jointly (or 'in conjunction' with each other).

The relevant stakeholder must always be consulted when section 23 or section 24 exemptions are being considered, so a referral to the NPFDU is mandatory. This procedure must be

followed whether the data is held or, if not, would likely have come from a s23 body.

National Security

The test to be applied when considering whether to claim the section 24 exemption is not whether the information relates to national security but whether the exemption is required for the purpose of safeguarding national security. That is, to claim the exemption it must be possible to identify the risk of an undesirable effect on the national security of the UK and its citizens.

There is no definition of 'national security' in the Act, however in the IT EA/2006/0045 it was recognised that "national security" means:

- the security of the United Kingdom and its people;
- the interests of national security are not limited to actions by an individual which are targeted at the UK, its system of government or its people;
- the protection of democracy and the legal and constitutional systems of the state are part of national security as well as military defence;
- action against a foreign state may be capable indirectly of affecting the security of the UK;
- and reciprocal co-operation between the UK and other states in combating international terrorism is capable of promoting the United Kingdom's national security.

Section 24 applies where withholding the information is 'required' for the purposes of safeguarding national security. "Required", is taken to mean that the use of the exemption is 'reasonably necessary'. "Necessary" in this context is taken to mean something less than absolutely essential but more than simply being useful or desirable. It is not sufficient for the information to simply relate to national security, it must be clear that disclosure would have an adverse effect on national security.

NCND existence of information

Careful consideration is required when assessing the need to confirm or deny matters exempt by way of section 23 and section 24, individually or combined. Further guidance can be found on the Neither Confirm Nor Deny principles within this manual.

Where responses are considered for information relating to exempt bodies or national security purposes, in most cases it will be necessary to assess adopting an NCND approach: 23(5) and/or 24(2). The duty to confirm or deny does not arise if to comply would itself disclose information, which is exempt under the Act. The use of section 23 and section 24 together may be the only way that the 'non-committal' response that NCND requires in order to work, may be maintained. This is so that it cannot be readily inferred that use of the two exemptions together is itself an indicator of the relevant security body activity, it is also important that where section 24 is relied on, reciprocal consideration is given to the justification for relying on section 23.

To apply section 24(2), it is sufficient to demonstrate that either a hypothetical confirmation or a hypothetical denial would engage the exemption. It is not necessary to show that both

potential responses would engage the exemption.

In assessing whether section 24 applies, the Commissioner may need to have access to the information that is held, although she may be satisfied with confidential discussions with experts in the relevant area.

Ministerial Certificates

Occasionally at the point of an ICO appeal or Information Tribunal (IT), 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 NPFDU in close consultation with the Ministry of Justice (MOJ) and relevant stakeholder agencies. Section 60, as mentioned in the legislation allows for the commissioner or an applicant to appeal the application of a ministerial certificate.

SECTION 26 DEFENCE

LEGISLATION

****S21(1) Information Reasonably Accessible by other means****

GUIDANCE

The term 'co-operation' may include:

- Working with the UK's forces on a particular project or to include a much wider range of 'friendly' forces; and
- Information about the capabilities and vulnerabilities of forces working with UK forces.

The effect of disclosing information on the relationship between the UK and any other state should also be considered as a relevant factor in the public interest test when applying this exemption.

The following are examples of information which might be covered by the exemption:

- Policy and strategy, planning and intelligence;
- Operational orders, tactics and rules of engagement;
- General capability and effectiveness, for example the performance of troops or military equipment and weaponry;
- Plans and measures covering:
 - the maintenance of essential supplies and services needed for military operations
 - military capabilities, current and future, including access to and availability of weaponry; and defence or reinforcement of other countries including an formal or informal arrangements and agreements

- Less clearly related information such as details of fuel and other important supplies, and the location of telecommunications equipment and military transport.

The NCND element is at section 26(3) and the public authority must be able to demonstrate that confirming or denying information is held could pose a risk to defence matters or the safety of troops, or could assist an enemy.

The NPFDU feels this exemption will have limited application within the Police Service but it should be remembered that special forces are a s23 body under the Act.



SECTION 27
INTERNATIONAL RELATIONS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

THIS IS A MANDATORY REFERRAL TO THE NPFDU

GUIDANCE

Section 27(1) is prejudice-based and covers disclosures that would, or would be likely to, prejudice international relations.

Differences in culture, religion, legislature and infrastructure will determine the type and level of prejudice that may occur to the international relations between the UK and another state or states, international organisation or international court.

This is a broad exemption that is designed to cover the 'interests of the United Kingdom abroad' and 'the promotion or protection by the United Kingdom of its interests abroad'.

The exemption, however, does not cover the interests of specific groups within the state. Rather, this provision is designed to protect general national interests.

Information is exempt under section 27(2) and (3) if it is confidential information obtained from a state other than the United Kingdom, or from an international organisation or international court. Sections 27(2) and (3) relate not primarily to the subject of the information, nor the harm resulting from its disclosure, but to the circumstances under which it was obtained and the conditions placed on it by its supplier.

Since section 27(2) is class-based, there is no need for a public authority to establish the specific prejudice that would occur from disclosure.

The duty to confirm or deny the existence of information is also excluded to the extent that compliance with that duty would "involve the disclosure of any information (whether or not already recorded) which is confidential information obtained from a State other than the United Kingdom or from an international organisation or international court".

There is some overlap between section 27(2) and section 41 (Information in confidence). However, section 41 applies to the disclosure of information obtained from another person whilst section 27(2) refers to information obtained from a state, organisation or court that:

- Is confidential at any time while the terms on which it was obtained require it to be held in confidence; or
- While the circumstances in which it was obtained make it reasonable for the state, organisation or court to expect that it will be so held.

Section 27(3) refers to the expectation placed on the information by an international organisation, non-UK state or international court, that it will be held in confidence by the UK public authority. Section 27(3), therefore, includes implied confidence.

Changing events affecting international relations will also influence the application of the exemption to requests for the disclosure of information under section 27.

Forces might use a section 27 exemption in relation to requests regarding forces' international responsibilities (such as training), relationships with overseas forces or

organisations or in relation to requests surrounding the potential disruption to the United Kingdom following large issues of a legal and a political nature (such as the UK's withdrawal from the EU).

Section 27 may interact with other exemptions, most likely sections 23, 24 and 31 and if considered for use should be referred to the NPFDU for stakeholder approval

SECTION 28 RELATIONS WITHIN THE UNITED KINGDOM

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

This exemption was included in the Act to protect relations between the devolved administrations of the UK.

Devolution is now an established part of the constitution of the United Kingdom and the three Acts of Parliament (the Scotland Act 1998, the Northern Ireland Act 1998 and the Government of Wales Act 1998) define the respective functions of the UK government and the devolved administrations.

It is recognised that it is legitimate for different administrations to take a different view of a wide range of different matters and that from time to time these differences may give rise to disagreements which are the subject of negotiations, particularly between the UK administration and the devolved administrations.

Where the release of information would compromise these relations, this exemption may be applied.

Local Authorities throughout the United Kingdom are excluded from this section as are the administrations of the Isle of Man and the Channel Islands.

In contrast to section 27 (International relations), there is no specific class-based exemption covering information received in confidence from another administration in the UK.

It is NPFDU's view that this exemption will have very limited relevance to the Police Service.

SECTION 29 THE ECONOMY

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Categories of information that might fall within this exemption may include premature disclosure of governmental intentions relating to taxation or to the disposal of substantial property holdings owned by the state that would be likely to lead to the prejudice of the short-term economic interests of the UK. This exemption may also be used for information that would, if released, prejudice the economics of a region, in terms of inward investment for example.

It may be more difficult, however, for public authorities to prove that disclosure would cause prejudice in the longer term.

It is believed that section 29 will not be a key exemption for the Police Service.



**SECTION 30
INVESTIGATIONS AND PROCEEDINGS CONDUCTED BY PUBLIC
AUTHORITIES**

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

The Information Commissioner's Guidance on the section 30 exemption – [Investigations and proceedings](#)²⁵ details that subsection (1) can only be claimed by public authorities that have certain duties or powers to investigate offences and institute criminal proceedings. A duty is something that the public authority is obliged to do, whereas a power simply allows the public authority to do something. A public authority has discretion over whether it exercises its powers.

Section 30(1)(a) can only be claimed by a public authority that has a duty to investigate [offences](#). When citing section 30(1)(a) public authorities need to explain not only how the duty to investigate arises but also which offence or offences are relevant in the particular circumstances. The exemption applies to both investigations leading up to the decision whether to charge someone and investigations that take place after someone has been charged.

Any investigation must be, or have been, conducted with a view to ascertaining whether a person should be charged with an offence, or if they have been charged, whether they are guilty of it. It is not necessary that the investigation leads to someone being charged with, or being convicted of an offence.

Section 30(1)(a) will still protect information if a police investigation fails to establish that an offence has been committed, or concludes that there is insufficient evidence to charge anyone.

Section 30(1)(b) and 30(1)(c) are not used by the Police Service.

HISTORICAL RECORDS

Under section 63 of FOIA information contained in a historical record cannot be exempt under section 30(1). Originally, a historical record was one over 30 years old, or if forming part of a file, the last entry on that file must be over 30 years old. However, this has now been amended to 20 years by the Constitutional Reform and Governance Act 2010 which was phased in gradually over 10 years until it reached 20 years at the end of 2022.

If this time period has expired and the information requested is deemed to be a historical record, then section 30(1)(a) is no longer available, however, information relating to criminal investigations held in a historical record could still be exempt under section 31(1)(a)(b) Law Enforcement if its disclosure would be prejudicial. Practitioners will still need to ensure that other exemptions such as section 40 are not still engaged

²⁵ [investigations-and-proceedings-foi-section-30.pdf](#)

SECTION 30(2) – CONFIDENTIAL SOURCES

Confidential sources are an important means of gathering intelligence about criminals and other offenders. A confidential source is a person who provides information on the basis that they will not be identified as the source of that information. Section 30(2) exists to protect these sources and ensure they continue to provide information to the authorities. The exemption is qualified and the need to safeguard the supply of such information is an important factor when considering the public interest test.

For information to be exempt under section 30(2) it must both relate to the public authority's investigations or proceedings **and** relate to confidential sources.

However, it does not have to be obtained or recorded as part of a particular investigation. It only has to be obtained or recorded by the public authority for the purposes of its functions relating to those investigations or proceedings.

Section 30(2)(b) relates to obtaining information from confidential sources.

Confidential sources (CHIS) include informants who are recruited by the authorities, often from within the criminal community, to provide intelligence on criminal activity.

These informants provide information secretly and have an expectation that the authority would keep their relationship confidential.

Confidential sources can also include witnesses who provide information to the police on the understanding that their identity would not be revealed having declined to give a formal statement.

Confidential sources will mainly be third parties. The exception to this is likely to be police officers and others working for law enforcement agencies who provide intelligence whilst performing an undercover role. These officers can only operate effectively and safely if their true identities remain unknown. As such the Information Commissioner is satisfied that they are confidential sources for the purposes of section 30(2).

RELATIONSHIP WITH SECTION 31

There are areas of overlap between section 30 and section 31. Whereas section 30 provides an exemption in relation to a particular criminal investigation, section 31 provides for general steps taken in relation to law enforcement.

It is clear within section 31 itself that where section 30(1)(a) applies section 31(1)(a)(b) cannot be used. This should be borne in mind when analysing investigation material subject to a request. All the information may not be covered by 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 section 31(1)(a)(b) instead, if the disclosure would prejudice law enforcement.

ATTRACTION OF NCND WHEN S30 IS ENGAGED

There is an option within section 30 to Neither Confirm Nor Deny the information is held.

The success of many investigations depends on ensuring the information is not disclosed prematurely.

It is likely that a non-committal response will be required when the existence of an investigation is not yet in the public domain or it is a necessary response to protect the identity of some informants or defendants.

For example a request stating 'please disclose copies of the investigation into Smith' whether held or not is likely to attract an NCND response, unless such an investigation is already public knowledge. To use exemptions or state 'not held' could actually disclose sensitive and personal information.

THE PUBLIC INTEREST TEST

Section 30 is a qualified exemption. This means that even if the information requested is exempt, the public interest in maintaining the exemption may be outweighed by a wider public benefit in disclosure.

A critical issue is likely to be the timing of the disclosure. Factors favouring disclosure are likely to be weaker while an investigation is being carried out, or is unsolved and subject to Criminal Procedures and Investigations Act (CPIA) review, for the reasons outlined above. However, once an investigation is completed, the public interest in understanding why an investigation reached a particular conclusion, or in seeing that the investigation has been properly carried out, could well outweigh the public interest in maintaining the exemption.

This will still be relative to the factors outlined in the public interest chapter; however, the ICO has the view that cases where justice was not done, either to the accused person or victim, may shift the public interest towards disclosure. This is especially so in cases where procedural failure or mismanagement is the cause.

CASE-BY-CASE

An important element when dealing with requests for investigations is the requirement to deal with each request on a case-by-case basis. Also, there is a need for each piece of information to be assessed. Simply applying a 'blanket' exemption because the information requested is an investigation, is not valid. Decision Notices and tribunal cases have shown that this is flawed because the PIT may well be different for each piece of information. For example a benign note on the file discussing charging options will have different considerations to a sensitive witness statement. The most cost and time effective method to do this will be to establish exactly what information the applicant really wants, potentially removing the need to analyse each separate piece.

It has been established from the Information Tribunal that even though section 30 is a class-based exemption, there is a requirement to clearly demonstrate in any refusal, what prejudice the investigation would suffer if the information were to be disclosed.

SECTION 31
LAW ENFORCEMENT

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 31 creates an exemption from the right to disclose information if releasing it would, or would be likely to cause significant harm to the functions of a public authority.

Public authorities may engage this exemption firstly either in relation to certain 'activities' listed under sections (1)(a) to (f), of the exemption which are:

- (a) The prevention and detection of crime.
- (b) The apprehension or prosecution of offenders.
- (c) The administration of justice.
- (d) The assessment or collection of tax.
- (e) The operation of immigration controls.
- (f) The maintenance of security and good order in prisons.

or secondly carrying out a 'specified purpose', section (1)(g) to (i) as outlined in section 31(2):

- Determining whether a person has broken the law;
- Determining whether a person is responsible for improper conduct;
- Determining whether there are or may be circumstances which would justify regulatory action;
- Determining a person's fitness or competence to manage a corporate body or to continue in any profession or other activity which they are or would like to become authorised to carry on;
- Determining the cause of an accident;
- Protecting charities against misconduct or mismanagement in their administration or recovering the property of charities;
- Securing the health, safety and welfare of staff: and
- Protecting people other than staff against risk to health or safety arising from the actions of a person's staff.

The use of this exemption by the Police Service is somewhat simplified due to the fact that it obviously carries out all of the activities of the prevention and detection of crime and the apprehension or prosecution of offenders listed under (a) and (b). The Information Commissioner's Guidance on the section 31 exemption stipulates that section 31(1)(c) cannot

be used by the Police Service as the administration of justice is not a core police function. This exemption can be used by a wide range of judicial bodies, such as courts, coroner's courts and tribunals, for disclosures that would in any way interfere with their efficiency and effectiveness, or their ability to conduct proceedings fairly.

The Police Service also has limited exposure to the activities outlined in (e) and (f) where policing involves the physical security of entry points to the UK or the external security of prisons. The Service has no functions that would involve the activities in (d).

The three remaining exemptions provided by section 31(1) are engaged by reference to subsection 31(2). The exemption being section 31(1)(g). When citing this exemption the subsection under section 31(2) must also be cited.

An example of when section 31(1)(g) by virtue of section 31(2)(b) is cited is with regard to police misconduct files where the investigation has been carried out purely for the purpose of ascertaining whether any person is responsible for any conduct which is improper.

It will be for decision-makers to establish whether the disclosure will or be likely to prejudice one of these activities, so that section 31(1) is correctly considered. If a specified purpose is likely to be compromised by disclosure, section 31(2) will be engaged instead. It will be rare for the latter to be used as the Police Service obviously carries out a law enforcement function as an activity, which is an established fact. However, practitioners still need to understand the differences between 'activities' and 'specified functions' as the use of this exemption is not restricted to those authorities whose information is simply covered by it, as is the case with section 30.

For example a local council may be asked for information that damages a police function, enabling them to engage the exemption legitimately. This is particularly relevant when reviewing information which has been generated by, or mutually shared, as part of partnership working.

WHAT TYPE OF INFORMATION IS COVERED?

The information potentially covered by this exemption is very broad. As a general, but not exhaustive guide, consideration should be given to any disclosure which will or could prejudice:

- Crime prevention, detection or reduction.
- Arrest or prosecution of offenders.
- Penalties for criminal behaviour.
- Breaches of military law.
- Administrative arrangements of courts.
- Court functions.
- Witness care.
- Transport of defendants.
- Civil case processes.
- Effective and efficient conduct of a police force or the service.
- Security and protection arrangements.

RELATIONSHIP WITH SECTION 30

There are areas of overlap between section 30 and 31. It is mandated within section 31 itself that where section 30 applies to information, then section 31 cannot also be engaged. So although these two exemptions cannot be applied to the same piece of information, there may be a need to still use both exemptions in response to a request. It is imperative, therefore, that an applicant is told exactly which exemption is relevant to which part of the information.

For example, a request for information in relation to an investigation is received. The request asks for information about the decision-making process behind key decisions in the investigative process. It would appear that section 30 is engaged and therefore section 31 is excluded. However, examination of the case papers shows that various procedural documents and Manuals of Guidance are also relevant to the request, not just the case papers. Since section 30 only covers *'Information held by a public authority if it has at any time been held by the authority for the purposes of any investigation which the public authority has a duty to conduct'*, This will cover the case papers but not the other documents. If the disclosure of the additional documents will or be likely to prejudice law enforcement, then section 31 will also be engaged for these documents.

ATTRACTION OF NCND WHEN SECTION 31 IS ENGAGED

There is an option within section 31 to Neither Confirm Nor Deny the information is held. An example where a force may wish to NCND using section 31 would be where a particular tactic is not widely known in the public domain and is therefore likely to attract a non-committal, NCND response to ensure policing methods are not undermined.

HARM AND THE PUBLIC INTEREST TEST

Section 31 is a qualified and prejudice-based exemption. This requires the production of evidence of the prejudice that may be caused by disclosure and a full public interest test. A critical issue is likely to be the timing of the disclosure. Factors favouring disclosure are likely to be weaker while a tactic or methodology is still in current use. However, great care still needs to be taken as it is not uncommon for an outdated tactic to be bought back into use, sometimes many years later, as criminals modify their behaviour.

Information covered by this exemption also tends to attract the most difficult public interest balance test. There is an argument that there is a public interest in knowing why something was done, particularly if it were badly managed, a procedural failure or mismanagement being the cause, and the ICO has outlined their view that cases where justice was not done, either to the accused person or victim, may shift the public interest towards disclosure.

Each request must be dealt with on a case-by-case basis. There is a need for each piece of information to be assessed. Simply applying a 'blanket' exemption because the information requested would prejudice law enforcement is not valid. The most cost and time effective method of achieving this detailed assessment is to establish exactly what information the applicant really wants, potentially removing the need to analyse each separate piece.

HISTORICAL INFORMATION

This exemption does not apply to information in records that are more than 100 years old.

SECTION 32 INFORMATION CONTAINED IN COURT RECORDS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Although large amounts of police information are submitted to the courts, the majority of this information is unlikely to be covered by the section 32 exemption.

This is due to the key words used within the legislation which stipulate that information held **'only by virtue'** is covered. The ICO guidance states that:

The information covered is that which is held “only by virtue” of being contained in any documents which have been: served upon or by a public authority, for the purposes of court proceedings.

However, it also states that:

*The phrase, “only by virtue of,” implies that **if** the public authority also holds the information elsewhere it may not rely upon the exemption. For instance, a public authority may have a set of financial records which are the subject of litigation. If those records are held only for the purposes of litigation and are contained in court records, then they are exempt. However, if it also held the records for another business purpose (e.g. the authority’s obligation to keep financial records) then they would not be exempt.*

The reasoning behind the exemption appears to be that it would be undesirable to interfere with existing court rules regarding access to information i.e. that a party to proceedings will have rights of access to information under the normal disclosure rules.

Police information is rarely gathered solely for court use as it tends to have multiple functions. In fact, it is unlikely at the information-gathering stage that a definitive knowledge as to the likely final use of the information would be known. For example witness statements are taken as the police service has a statutory function to investigate crime and secure evidence. However, at the time statements are taken, the future or end usage of that information is unlikely to be known.

In any case, information relating to forthcoming criminal or civil litigation cases is not covered by this exemption. The proceedings in question must have already commenced or have been concluded at the time the request was received for section 32 to be engaged. It therefore cannot be applied to proceedings which may be contemplated.

Anything generated by the court itself will attract this exemption in addition to anything produced by the police solely for court use. Discovering the provenance and reasons for the existence of information is key to identifying whether this exemption may be engaged.

An example of section 32 being upheld by the ICO is [DN FS50611169](#)²⁶ which relates to a report compiled by the force in response to a report from the Coroner’s Office. A further example may be victim impact statement which may be held by the force but compiled solely for use by the courts.

²⁶ [fs50611169.pdf](#)

SECTION 33 AUDIT FUNCTIONS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

This exemption may be cited by public authorities that have functions relating to either:

- The audit of accounts of other public authorities; or
- To the examination of the economy, efficiency and effectiveness with which other public authorities use their resources in discharging their function.

Importantly, this exemption **does not** cover information that relates to a local authority's internal audit.

NPFDU guidance is that this exemption may be used for information that's intended for future publication where the public interest test has been applied and it is judged that there may be an adverse effect if the information requested is released prematurely.

This exemption is designed to protect organisations with an external audit function – such as the Audit Commission or Her Majesty's Inspector of Constabularies (HMIC) – where the audit results are, by their very nature, for public consumption.

This exemption **does not** cover auditing processes that an organisation may exercise on itself, internally.

SECTION 34 DISCLOSURE WHICH WOULD INFRINGE PARLIAMENTARY PRIVILEGE

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Information is exempt from disclosure if its release would infringe the privileges of either House of Parliament.

The purpose of this exemption is to protect Parliament's power to retain control over disclosure of its own information.

The duty to confirm or deny is excluded under this exemption where confirming or denying the existence of information would infringe the privileges of either House.

Whilst confirmation or denial of the existence of information is less likely to infringe Parliamentary privilege than disclosure itself, section 34(2) will apply where confirmation or denial would result in a breach of privilege.

SECTION 35 FORMULATION OF GOVERNMENT POLICY AND OTHER GOVERNMENTAL INTERESTS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

This is not an exemption that the Police Service can apply: its use is limited to government departments

This exemption was incorporated into the Act to ensure that policy discussion can be conducted privately. Without this protection, the 'normal' processes of government may be inhibited. Civil servants, for example, may be less candid in their advice to Ministers when considering policy options.

This exemption is reasonably broad in its scope and can be used to cover the formulation or development of government policy even where a policy has been finally adopted.

Limitations on the scope of this exemption have been introduced. For example, once a decision on government policy has been made, background statistical information that provided an

informed background in the decision-making process does not fall under this exemption and may therefore be subject to disclosure.

ICO Guidance recommends the disclosure of factual information used to underpin the decision-making process.

Whilst this exemption is wide-ranging, it is not all-encompassing and covers only information relating to the 'formulation or development of government policy'. Information that relates to the execution of adopted policies or information concerning other procedural or administrative functions will not fall within the exemption.

**SECTION 36
DISCLOSURE PREJUDICING THE EFFECTIVE CONDUCT OF PUBLIC
AFFAIRS**

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Information is exempt from disclosure if, in the reasonable opinion of a 'qualified person', its disclosure would prejudice, or would be likely to prejudice, certain specified interests relating to public affairs. Section 36 requires that, other than for statistical information, the qualified person for the public authority must give their reasonable opinion that the exemption is engaged.

A specific definition of a 'qualified person' is not included in the Act. For the Police Service, the suitably 'qualified person' is the Chief Constable or Commissioner.

Section 36 differs from other exemptions because it uses the term 'reasonable opinion.' Information to which this section applies is exempt information if, in the reasonable opinion of a 'qualified person', disclosure of the information:

- (b) would, or would be likely to, inhibit
- (i) the free and frank provision of advice, or
- (ii) the free and frank exchange of views for the purposes of deliberation, or
- (c) would otherwise prejudice, or would be likely otherwise to prejudice, the effective conduct of public affairs.

Interestingly, the qualified person's opinion does not have to be the most 'reasonable' opinion. What is important however, is that the evidence and audit trail prove that the opinion is reasonable. Many factors may come into play when consideration is given. For example, the nature of the information and timing of the request for an ongoing issue which requires the free and frank exchange of views. Many forces experienced such an issue in the early austerity years with a high number of requests asking about 'force mergers'. The concern was that FOI would undermine forces' ability to review/plan for mergers and would cause unrest amongst the workforce in relation to redundancy.

Section 36 is a qualified exemption and the public interest test is crucial with this exemption. Although the qualified person may consider that one of the subsections are engaged (and it is important to quote the relevant subsection), it may fail under the public interest and be released.

A decision made under section 36 needs to be able to stand intense scrutiny. Any information needs to be assessed on a 'case by case' basis depending very much on the subject matter, the harm identified and the public interest.

Circumstances where section 36 has been considered for requests under FOI within forces are in relation to 'if asked' media statements. For example, media statements may have been prepared as part of a contingency planning process for major incidents. Disclosure could prejudice your forces ability to carry out your functions should the incident occur, as it could impair the quality of decision making.

Under this exemption, there is also no duty to confirm or deny if, in the opinion of 'reasonable person,' the information is not disclosable. Again, it is essential that the rationale is recorded that to even confirm or deny that any information is held would in itself have the effects listed in section 36(2). A public interest test is still required.

Where section 36 is engaged in respect of information held by the House of Commons or House of Lords, the exemption is absolute.

The ICO website published a [template form²⁷](#) to use when providing information to them when they are investigating a section 50 Appeal.

Section 36 does not apply to historical records (those over 30 years old (now amended to 20 years, being phased in) except in Northern Ireland where the time limit remains at 30 years.

With regard to section 36(4) a qualified person's opinion is not required however, the force will need to articulate why the information is being withheld (as in section 36(2)). The term "statistical information" is more than just statistics, it covers raw data used for analysis and the methods used to reach the analytical conclusion.

²⁷ [Section 36: Record of the qualified person's opinion | ICO](#)

SECTION 37

COMMUNICATIONS WITH THE ROYAL FAMILY AND HONOURS –
ICO Guidance has reflected the Queens passing and has changed the title to:
COMMUNICATIONS WITH HIS MAJESTY AND THE AWARDING OF
HONOURS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

THIS IS A MANDATORY REFERRAL TO THE NPFDU

GUIDANCE

This exemption is both qualified and absolute, depending on the communications requested. This has not always been the case; prior to January 2011, all the provisions of section 37 were qualified. The change was made in line with the Constitutional Reform and Governance Act 2010, which introduced subcategories that do not require further qualification.

This exemption covers communication, i.e. letters or other documents, with members of the Royal Family or Royal Household. It will also apply to notes of meetings between officials of a public authority and a member of the royal family or royal household. It also covers information relating to the awarding of honours and dignities by the crown.

Section 37 can only be applied within legislative timescales:

- 5 years from the date of the “relevant death”
- 20 years from the date the information was created.
-

“relevant death” references the death of the individual to whom the communication relates.

- Section 37(1)(b) is only applicable for information under 60 years old.

NPFDU guidance is that all communication falling under this exemption will be actively protected. Where a request is received in relation to the Royal Family and/or any policing issues associated with them, the request must be referred to the NPFDU.

SECTION 38 HEALTH & SAFETY

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

A section 38 exemption may be applied where disclosure of information would, or would be likely to endanger:

- The physical or mental health of any individual; or
- The safety of an individual.

By applying this exemption to 'any individual', it may be interpreted as the mental or physical health of a police officer, the requester, another individual, a family member of a victim, or the public in general.

It is likely therefore that this definition will cover a wide spectrum of scenarios, however care should be taken in the use of this exemption as it is one of the weakest exemptions due to the amount of evidence that is required to satisfy the ICO of its suitability.

This exemption is in line with a similar provision in the Data Protection Act (DPA) that prohibits subject access where there is a risk of 'serious harm'. However, under FOI there must be 'a real and significant risk' in order for this exemption to apply. In other words, there must be actual evidence of the harm that would occur if the information was disclosed.

This exemption may cover information relating to:

- scientific research where disclosure could lead to sabotage and there would be risks to the physical safety of staff,

- someone who has died, where disclosure might endanger the mental health of surviving relatives, particularly if they had been unaware of it,
- an issue where disclosure might have an adverse effect on public health (for example, research into the safety of a particular medication),
- the identity of informers or undercover officers,
- any plans or policies relating to the accommodation of individuals, or groups of individuals where disclosure could lead to them being threatened or harassed (for example asylum seekers, ex-offenders);

Other areas that would be protected under section 38 are photographs and videos showing post-mortems, injuries, accidents, crime scene videos and similar material that would be likely to affect the mental health of those affected if released into the public domain.

Section 38 will most often be used to protect the identities of CHIS, RSO's, those under witness protection or police protection, and police officers addresses (and sometimes their identity), because, for all of these circumstances, there are vast amounts of evidence of the harm that would actually be caused by disclosure.

The word 'endanger' is used rather than 'prejudice' because it is more meaningful in the context of an individual.

SECTION 39 ENVIRONMENTAL INFORMATION

LEGISLATION

S21(1) Information Reasonably Accessible by Other Means**

GUIDANCE

This exemption aims to ensure that any requests for information are handled under specific regulations implementing the UK's international obligations on access to environmental information rather than under the FOI Act.

Where a request for environmental information is made, it should be considered under the Regulations rather than under the FOI Act and section 39 provides this exemption. If a request for environmental information is dealt with under the EIR, then the ICO would not expect a FOIA refusal notice to be issued.

NPFDU suggests mechanisms should be in place to automatically route queries relating to environmental information through the Environmental Information Regulations.

For more information, please see Appendix 1.



SECTION 40
PERSONAL INFORMATION

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 40 for the most part is an absolute exemption. When assessing the applicability of s40, these questions will need to be addressed:

1. *Is the information 'personal data' or involve any of the special categories of personal data?*
2. *Whose is the personal data? Is it the applicant's or another third party?*
3. *Would disclosure breach one of the data protection principles?*

1. Is the information 'personal data' or involve any of the special categories of personal data?

As defined by [Article 4\(1\) of the GDPR²⁸](#) personal data' relates to a living individual who can be identified directly from the information, or identifiable indirectly in combination with other

²⁸ [Art. 4 GDPR – Definitions - General Data Protection Regulation \(GDPR\)](#)

available information.

This definition also includes an expression of any opinion or indication of intentions relating to the individual. The ICO provides further guidance on [what is personal data.](#)²⁹

There are categories of personal data that are considered more sensitive and require more protection.

- 'Special Category Personal Data' is information relating to protected characteristics like race/ethnicity, religion, political and philosophical opinion, biometric and genetic data, mental/physical health, sex life or sexual orientation, and trade union membership.
- 'Criminal Offence Data' relates to criminal convictions, offences or related security measures, including criminal proceedings and sentencing.

It is important to recognise when an applicant makes a request involving the above 'sensitive' information to ensure the highest level of scrutiny is applied before any potential disclosure can be justified.

2. Whose is the personal data? Is it the applicant's or another third party?

S40(1)

Where a request is made by an applicant for their own personal information, they are the data subject and this is an absolute exemption.

Requests for a person's own personal data are often made incorrectly quoting FOI. There is no requirement to specify the particular legislation when making the request. It is up to the authority receiving the request to determine the correct path.

Data subjects have the right to request access to their own personal information under data protection legislation (Article 15 of the GDPR and s45 of the DPA).

A Right of Access Request (RoAR) (previously known as a Subject Access Request or SAR) is the correct route for this disclosure and should be channelled through to the appropriate team, with a section 40(5) refusal notice issued.

S40(2)

Where the applicant makes a request for information including third party personal data (not their own), it is an absolute exemption under section 40(2) if disclosure would breach any of the data protection principles. The EIR has an equivalent exemption.

3. Would disclosure breach one of the data protection principles?

Personal data should be processed in the below ways to comply with the data protection principles:

Principle 1: Lawful, Fair and Transparent

- Disclosure must not breach any statute, law or regulations.

²⁹ [What is personal data? | ICO](#)

- Disclosure should be reasonably expected by the data subject and not cause any adverse impact on the data subject.

NOTE: *fairness is probably the most important consideration for FOI disclosure. Would disclosure of the third party's personal data be fair to them? See below for more detail.*

- We should be clear, open and honest about how we use people's personal data.

Lawful

In order for a disclosure under FOIA to be lawful, one of the lawful bases in [Article 6\(1\)³⁰](#) of the GDPR must apply to the processing. It must also be generally lawful. The IC considers subsection 6(1)(f) "Legitimate Interests" to be the most applicable.

In considering the application of Article 6(1)(f) it is necessary to consider the three part test:

- **Legitimate Interest Test:** Whether a legitimate interest is being pursued in the request for information. Legitimate interests can include broad general principles of accountability and transparency.
- **Necessity Test:** Whether disclosure of the information is necessary to meet the legitimate interest in question. Disclosure under the FOIA must be the least intrusive means of achieving the legitimate aim in question.
- **Balancing Test:** Whether the above interests override the legitimate interest(s) or fundamental rights and freedoms of the data subject. Once established that disclosure is necessary to meet the legitimate interest, you should consider the impact of disclosure, considering any harm or distress, what is already in the public domain, expectations of the individual etc.

Fairness

Public authorities should consider the expectations of the data subject, and whether disclosure of information would be considered reasonable. For example;

- **Seniority of role**

The more senior the data subject's position, the less unfair is it to disclose certain types of information e.g. The number of complaints made against the CC. In the [DN FS50618842³¹](#) the ICO states that given the seniority of the rank it would not be unreasonable that the public interest requires transparency about complaints in the CC professional role.

- **Public facing role**

If the data subject is responsible for explaining and defending policies or actions to the world, there is a lower expectation of privacy.

- **Decision making**

If the data subject is making decisions around expenditure, policy or operational decisions then there is a reasonable expectation towards disclosure.

³⁰ [Art. 6 GDPR - Lawfulness of processing - GDPR.eu](#)

³¹ [fs50618842.pdf](#)

- Private life vs public life

An example of this crossover situation relates to vehicles paid for by the force for business and personal use by some senior officers, in which case there is a reasonable expectation of disclosure.

- Public domain

If individuals have placed information into the public domain themselves, then this would undermine any argument that it would be unreasonable to disclose the same personal information under FOI.

In summary, if the disclosure of personal data under FOIA or EIR is considered to be lawful, fair and transparent, then it does not contravene the first data protection principle and release of the information can be considered.

Principle 2: Purpose Limitation

- Only use the data for a new purpose if it's compatible with your original purpose, you have a clear obligation or it is required by law (FOIA).

NOTE: Compliance with the terms of FOIA is a statutory obligation. This means that forces may need to process personal data in order to extract the information that has been requested. This would not represent a breach of data protection legislation, even though the force is not now processing the data for reasons for which it was originally gathered e.g. accessing PNC.

Principle 3: Data Minimisation

- Disclose the minimum amount of personal data necessary to fulfil the purpose.

NOTE: Consider redaction or anonymization of personal data that is not necessary to disclose.

Principle 4: Accuracy

- Take reasonable steps to ensure that the personal data you hold is not incorrect or misleading.

Principle 5: Storage Limitation

- Personal data must be kept for no longer than is necessary.

Principle 6: Integrity and Security

Have in place appropriate security measures to protect the data you hold to ensure its 'confidentiality, integrity and availability'.

Section 40(3A)(a) would be engaged if any of the data protection principles were to be breached. If you are refusing the information under this sub-section, it is a requirement to articulate to the applicant which of these principles would be breached, and why.

Section 40(3A)(b) covers manual unstructured data held by Public Authorities, this is hard-copy personal data which is held on paper. The GDPR and section 21 of the DPA cover personal data processed wholly or partly electronically and manual information in a filing system. Section 21

DPA 2018 extends this to cover personal data processed by manual unstructured processing. The purpose being to protect this personal data in FOI disclosures.

Section 40(3B) would be engaged if the data subject has exercised their right to object to processing (under [Article 21 of the GDPR³²](#)) and the objection was accepted. The exemption is not engaged if the objection is received at the time of the FOI request.

Section 40(4A) provides exemptions for personal data if said data is exempt from disclosure under a Right of Access Request. If the data would not be released to the data subject as part of a RoAR under GDPR or DPA, then it should not be given to a third party making an FOI request. A public interest test will apply, and if it results in favour of disclosure the information can be disclosed, provided this is not in contravention of the data protection principles.

- Section 40(4A)(a) is engaged if the personal data has been processed under the GDPR for general purposes, for instance Human Resources processing employee information
- Section 40(4A)(b) is engaged if the personal data has been processed under Part 3 of the DPA for law enforcement purposes, for instance criminal records, personal information relating to police investigations etc.

This is further explained within the [ICO Guidance, What should we do if the request involves information about other individuals?³³](#).

NCND application

Section 40(5A) applies if the information being requested is that of the applicant. The applicant should be advised to submit a Right of Access Request (RoAR) to the relevant force from which they require their personal information.

Section 40(5B) (a-d) applies if:

- It would contravene the data protection principles.
- It would contravene an objection to processing.
- The information (i.e. the confirmation or denial) is exempt from the subject access right.

If the duty to confirm or deny contravenes the first principle, then the exemption is absolute. In respect of the other conditions above, the exemption is qualified and requires a public interest test.

Further information can be found on the ICO website [Personal Information³⁴](#).

³² [Art. 21 GDPR – Right to object - General Data Protection Regulation \(GDPR\)](#)

³³ [What should we do if the request involves information about other individuals? | ICO](#)

³⁴ [Section 40 and Regulation 13 – personal information | ICO](#)

SECTION 41 INFORMATION PROVIDED IN CONFIDENCE

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 41 covers information provided in confidence and is likely to have widespread relevance to the police service. However, whilst the exemption appears to be both class-based and absolute, its power is reduced because it is defined in 'relation to the equitable action for breach of confidence'.

This means section 41 is an absolute exemption - where release of the information would result in an actionable breach of confidence - but it has its own built-in form of testing for ascertaining whether there could be such a breach.

This exemption does not cover information that a public authority has generated internally. It specifically relates to information that has been obtained by the public authority from another person (this may include an individual, a company, a local authority or any other 'legal entity'), that has been externally generated.

The exemption may be enforced only where an actionable breach of confidence would occur should the information be disclosed. This is where release would result in the provider or a third party taking the authority to court.

Information falling within section 41 may also be exempt from disclosure under section 40 (Personal information), Section 43(Commercial interests) or section 30(2) (Confidential sources)

What is confidentiality?

A duty of confidence arises when one person (the confidant) is provided with information by another (the confider) in the expectation that the information will only be used or disclosed in accordance with the wishes of the confider.

In trying to determine whether an obligation of confidence has arisen in a particular case, consideration should be given to:

The circumstances under which the information was provided.

When the confider provides information to the authority, explicit conditions are attached to its subsequent use or disclosure. This may take the form of a contractual term or may be stated, for instance, in a letter. Conditions are not stated explicitly, but are obvious or implied from the circumstances. For instance a patient does not need to tell a doctor not to pass on their information to a journalist, it is simply understood that these rules exist.

The nature of the information

Information which is protected from disclosure by an obligation of confidence must have the necessary "quality of confidence". There are two key elements to this:

- The information need not be highly sensitive, nor can it be trivial. The preservation of confidences is recognised by the courts to be an important matter and one in which there is a strong public interest. This notion is undermined if it is argued that even trivial matters are covered. However, otherwise trivial information may not be considered trivial if it relates to personal matters and the confider considers it important.
- The information must not be readily available by other means. Information which has been reported in the press or a chemical formula which can be worked out by any chemical analyst, for instance, are unlikely to be viewed by the courts as being confidential. On the other hand, it is not necessary that the information is completely secret. A patient does not lose the right to medical confidentiality, for instance, simply because he or she has given details of their condition to an employer or a friend.

When can confidential information be disclosed?

The duty of confidence is not absolute and the courts have recognised three broad circumstances under which confidential information may be disclosed.

Disclosures with consent.

Disclosures which are required by law.

Disclosures where there is an overriding public interest.

Actionable breaches of confidence

Public authorities relying on section 41 must be satisfied that any breach of confidence would be actionable. If there is any doubt it may be necessary to take advice, including from the person affected. In addition the aggrieved party must have the legal standing to take action.

Continuation of confidentiality after death

It has been confirmed by the Information Tribunal that the duty of confidentiality does continue after the death of an individual to whom that duty is owed. Where there is a legally enforceable duty of confidentiality owned by a living individual, after death it can be enforced by the deceased's personal representative. This is particularly relevant to public authorities holding records on an individual's personal details. An example of this with regard to police forces would be information gathered from a detained person to compile a custody record and other personal information gathered as part of an investigation, e.g. banking details.

Breach of confidence test

To determine whether a breach of confidence would occur if the information were to be disclosed, the following questions need to be applied:

Does the information have the necessary quality of confidence about it?

Information that is already in the public domain, or has not been treated as confidential by the originator, does not have the necessary quality of confidence. Where information has been subjected to restricted disclosure – where it is not already available publicly or where the originator of the information has treated it as confidential – the information may still be subject to an obligation of confidence.

Was the information imparted in circumstances that imply an obligation of confidence?

This refers to whether the 'confider' of the information expresses that the information is confidential in nature when s/he imparts the information to others. At the same time, the recipient of the information must acknowledge that the information received is confidential in nature. In this case, there is an obligation of confidence attached to the information.

Was there an unauthorised use of that information to the detriment of the person communicating it?

This exemption also applies to information given to a public authority by another body or individual, not information that a public authority itself might consider as confidential. When deciding on whether to release the information or not, there is no obligation to consult third parties but the Codes of Practice state that those parties affected by disclosure should be approached.

SECTION 42

LEGAL PROFESSIONAL PRIVILEGE

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Under the Act, an applicant may not obtain disclosure of legal advice offered to a public authority by a solicitor in private practice or an in-house lawyer, subject to the application of the public interest test since this is a qualified exemption.

This exemption is class-based. This means there is no requirement to demonstrate any 'prejudice' that may occur to the professional legal adviser/client relationship if information is disclosed. It is inherently implied that the release of information that may appear trivial might undermine the relationship between lawyer and client. However, the public interest test must be applied to determine whether the information should be disclosed or exempted.

In the [Bellamy decision](#)³⁵ (EA/2005/0023, 4 April 2006), the Tribunal acknowledged that there are two types of privilege within the concept of LPP:

- litigation privilege; and,
- advice privilege

Litigation privilege applies to confidential communications made for the purpose of providing or obtaining legal advice about proposed or contemplated litigation.

Advice privilege applies where no litigation is in progress or contemplated. It covers confidential communications between the client and lawyer, made for the dominant (main) purpose of seeking or giving legal advice.

³⁵ [Bellamy v The Information Commissioner](#) | [2006] UKIT EA 2005 0023 | United Kingdom Information Tribunal including the National Security Appeals Panel | Judgment | Law | CaseMine

A communication under section 42 means a document that conveys information. It could take any form, including a letter, report, email, memo, photograph, note of a conversation, or an audio or visual recording. A document does not actually need to be sent for it to count as a communication for this purpose; a document that has been prepared to convey information, but is still on its creator's file, is still a communication.

Under section 63 of FOIA information contained in a historical record cannot be exempt under section 42. Originally, a historical record was one over 30 years old, or if forming part of a file, the last entry on that file must be over 30 years old. However, this has now been amended to 20 years by the Constitutional Reform and Governance Act 2010, so will reduce by a year, until it reaches 20 years at the end of 2022.

For the Police Service, section 30 (Investigations and proceedings conducted by public authorities) or section 31 (Law enforcement) may be more easily applied than section 42, Legal professional privilege.

When considering if communication with CPS would fall under LPP you will need to establish for each scenario if the CPS have acted as a legal adviser for the purposes of that advice as there will be some circumstances where they are not providing legal advice in the context of lawyer/client.

However, when police forces seek advice from the CPS in relation to a case, for example, to establish if there is sufficient evidence to charge a suspect (MG3 forms), then legal advice is being sought for the purposes of litigation and section 42 would be engaged.

NOTE: Where s42 is being considered or cited, the force's legal services department must be consulted.

SECTION 43 COMMERCIAL INTERESTS

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

Section 43 sets out an exemption from the right to know if:

(1) The information requested is a trade secret. A 'trade secret' is not defined in the FOIA, therefore making its interpretation broad. In reality an actual 'Trade Secret' is very hard to come by. Nevertheless if there is an actual trade secret in the forces possession, there is no need to apply the public interest test and consider the harm its release may cause. Section 43 does not absolve the authority from the obligation to inform an applicant whether it holds the information that constitutes a trade secret.

(2) The release of the information is likely to prejudice the commercial interests of any person (a 'person' may be an individual, a company, public authority itself or any other legal entity). Where the information requested does not constitute a trade secret, it can only be withheld if the public authority is satisfied a person's commercial interests would be compromised by its release.

Mandatory Publications (see appendix 5)

As part of the mandatory publication guidance, set out by the NPCC, forces are required to publish certain information that in some instances would negate any section 43 exemptions.

Forces are required to publish:

- Policies and procedures on procurement.
- Links to any sites where your force advertises contracts for tender.
- Details of contracts currently being tendered (that exceed £10,000).

- Current contracts whose value exceeds £10,000 and a list of those under £10,000.

The above information is required to be updated within 3 months of the contract being awarded. As contracts are meant to be regularly updated on the forces website this would place into the public domain current information that details company names, total/unit costs, length of contract etc. In the current climate it is expected that those third party companies who agree to supply products or services to public authorities should expect their details to be published with a view of being open and transparent as well as creating a competitive market.

If the information requested is not disclosed under the Publication Scheme the public authority is strongly urged to consult parties likely to be affected by the disclosure of commercial information to determine likely prejudice. Discussion with suppliers to identify the types of information that may harm commercial interests if disclosed may be appropriate. When considering prejudice to a third parties commercial interests, it will not be sufficient for the public authority to speculate about prejudice that may be caused rather arguments originating from the third party itself will need to be considered.

Therefore, in order to effectively engage Section 43 it is advisable to liaise with other parties in order to evidence their harm rather than what the force would believe the harm to be. It is, although, ultimately the responsibility of the public authority to decide whether or not an exemption applies to prevent the release of information.

It must be noted, when making a decision on whether commercial interests are affected, the ICO states that commercial interests does not always mean financial interests.

In order to evidence whether Section 43 will be engaged you will need to determine, but not exhaustively, these points below:

- Unit Costs
- Public authority's own commercial activities
- Policy development
- Policy implementation
- Private finance initiative/public private partnerships.
- Does the information relate to, or could it impact on commercial activity?
- Is the commercial activity conducted in a competitive environment?

The following outline some of the questions that may be asked when reviewing whether the release of information may harm the commercial interests of either the public authority or supplying companies:

- **Is the commercial activity conducted in a competitive environment?**
The lower the level of competition in any given marketplace, the less likely commercial interests will be prejudiced with the release of information. Where a public authority is the sole purchaser of specialist equipment, for example, the commercial interests of the

company could be more dependent on the procurement plans of the public authority rather than the impact of releasing commercial information.

- **Would there be damage to reputation or business confidence?**

If release were to damage a company's reputation or the confidence of customers, suppliers or investors, the commercial exemption may be applied. The same may be said where release may impact revenue or threaten ability to obtain supplies or secure finance.

- **Whose commercial interests are affected?**

In some circumstances, it may be unclear as to whose commercial interests may be prejudiced by disclosure of information. For example, if the amount of money set aside by a public authority for procurement is released, the bargaining position of the authority may be compromised if suppliers then increase their prices.

- **Is the information commercially sensitive?**

Companies compete by offering something different from their rivals. The difference will often be reflected in their price and may also relate to the quality or specification of the product or service they offer. Information identifying this unique element is likely to be commercially sensitive. It may also inadvertently reveal information about profit margins and possibly working practises.

It must always be considered whether the release of information is in the public interest, regardless of whether or not the information forms a trade secret. It is essential to weigh the possible prejudice caused by disclosure against the likely benefit to the applicant and the wider public.

In addition, just because a request for information was declined at one point in time, it does not mean that the public interest is best served if that information is permanently withheld. Market conditions may change and information relating to costs may become out of date quickly.

Contracts/confidentiality clauses

FOI decision-makers must also remember that there is an overlap between commercial interest and confidentiality. They will determine whether or not disclosure might prejudice commercial interests of a third party, consider the likelihood of a third party being able to successfully take action in the courts for breach of confidence.

During the procurement process, suppliers may request of public authorities that they sign confidentiality clauses that attempt to prevent the disclosure of information. However, 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 in the view of the ICO. Alternatively, clauses that seek to identify and protect that information that would genuinely prejudice a third party's commercial interests are perfectly acceptable.

Outsourcing

Difficulties can arise whereby Police Services are outsourcing functions such as Human Resources and Finance. It has been expected by companies who are supplying service on behalf of the Police, that due to the scale, complexity and substantial contractual costs that certain information would not be disclosed by forces. In some cases, there has been a reluctance to provide information which is considered not to be 'held' by them. Information created by staff employed by the contractor, on the forces behalf, would be held by the force for the purposes of FOIA.

What is important in these matters is that all of the parties involved cannot 'contract out' of FOI.

Public Interest

All Police forces are encouraged to be as open and transparent as possible. A factor that will always be considered with section 43 in the public interest test, in favour of disclosure, is how public money is spent. This is one of the reasons why the publication scheme has been implemented to routinely disclose expenditure by the forces. If a FOI request is received that is not covered in the publication scheme, how public money is spent becomes a very important factor in the balance test. Also, was the commercial project/ contract a success? If it was a failure, the public may have more of a right to know as public money has been spent. Although this may be embarrassing for the force, this is not an argument for non-disclosure, in fact quite the opposite.

SECTION 44 INFORMATION COVERED BY PROHIBITIONS ON DISCLOSURE

LEGISLATION

****S21(1) Information Reasonably Accessible by Other Means****

GUIDANCE

This exemption is something of a “catch-all” and states information that may be prohibited from disclosure under other legislation, is protected under FOI.

Under this exemption, information is exempt from disclosure if it is prohibited from being released under any other enactment.

Where there is another piece of legislation governing the release of certain categories or types of information, these are sufficient grounds to refuse release under an FOI request.

In effect, section 44 allows other pieces of legislation to be imported into the FOI Act under section 44.

Section 44(1)(a) prohibits information from disclosure under other legislation. Often referred to as statutory prohibitions or statutory bars, they prevent disclosure by public authorities if its disclosure would breach:

- primary legislation (an Act of Parliament); or
- secondary legislation (a Statutory Instrument).

Section 44(1)(b) prohibits disclosure of information if it is incompatible with or contradictory to any European Union legislation covering release of categories or types of information.

Section 44(1)(c) facilitates the withholding of any information that would, if released, lead to contempt of court.

For example, if a public authority were subject to a court order not to disclose particular information, this would be covered by section 44(1)(c) and disclosing it would be in contempt of court.

If the disclosure would be contrary to the Contempt of Court Act 1981 (CCA), this would be covered by section 44(1)(a) rather than section 44(1)(c).

If this exemption had not been included in the FOIA, there would be a danger that where there is a requirement for information to be withheld under other legislation, it may have been releasable under FOI, causing a potentially serious conflict without the protection afforded by section 44.

APPENDIX 1

ENVIRONMENTAL INFORMATION REGULATIONS

LEGISLATION

- 2(1) Environmental Information' has the same meaning as in Article 2(1) of the Directive, namely any information in written, visual, aural, electronic or any other material form on –
- (a) the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;
 - (b) factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a);
 - (c) measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements;
 - (d) reports on the implementation of environmental legislation;
 - (e) cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c); and
 - (f) the state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built structures inasmuch as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

GUIDANCE

The Environmental Information Regulations 2004 provide public access to environmental information held by public authorities in England, Wales and Northern Ireland. The regulations only apply to environmental information held, other types of information can be accessed using FOI.

The principles behind the regulations are being transparent and accountable, and providing the public with access to information and in turn greater awareness of issues that affect the environment.

The Regulations cover any recorded information held by public authorities which includes government departments, local authorities, the NHS, police forces and universities and also other bodies that carry out work that affects the environment.

The main differences between the FOIA and the EIR may be identified as follows:

- The key difference is that, unlike FOI requests, EIR requests may be received verbally and

there is no legislative requirement for them to be written down.

- Under FOIA, the public interest test applies only in the case of qualified exemptions. Under EIR the public interest test applies to most of the exemptions. However, Regulation 12(3) (personal data of a person other than the applicant) is not subject to the public interest test.
- Under EIR a pseudonym can be used when submitting an EIR request.
- There are additional exemptions under EIR that are not specifically covered under FOIA such as exemptions to disclose in relation to internal communications and exemptions on disclosure where release would adversely affect intellectual property rights or the protection of the environment. Under EIR, there are no exemptions that link the release of information with a prejudicial impact on the economic interests of the UK or part of the UK.
- Under EIR, the 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.
- Unlike FOI, EIR do not stipulate a requirement to adopt and maintain a publication scheme although there is a requirement to proactively publish this information. It is recommended that forces adopt and maintain a publication scheme with regard to EIR.

LIST OF EIR EXCEPTIONS

12(4)(a)	Information not held
12(4)(b)	Manifestly unreasonable requests
12(4)(c)	Requested formulated in too general a manner
12(4)(d)	Work in progress/Incomplete data
12(4)(e)	Internal communications
12(5)(a)	International relations, defence, national security or public safety
12(5)(b)	The course of justice and inquiries exception
12(5)(c)	Intellectual property rights
12(5)(d)	Confidentiality of proceedings
12(5)(e)	Confidentiality of commercial or industrial information
12(5)(f)	Adverse effect on the interests of the person who provided the information (subject to conditions) in regulation
12(5) (g)	Protect of the environment
12(6)	Neither confirm no deny
12(9)	Information on emissions
13	Personal information

All exceptions in regulations 12(4) and 12(5) are subject to a public interest test. The duty to provide information does not extend to an applicant's own personal data (regulation 5(3)), and personal data about other people can only be released subject to conditions in regulation 13, which exempts disclosure of personal data (as defined by the DPA) if it would contravene any of the data protection principles.

FREQUENTLY ASKED QUESTIONS

Which legislation does our request fall under, EIR or FOI?

Key points to assist public authorities

- If information is suitable for release there is no requirement to decide whether it is environmental or not – just provide the information.
- Each case must be treated on its own merits.
- The public interest test is the same whether the information is environmental or not.
- The definition of environmental information is wide. Careful attention must be paid to the wording of the definition and how the information requested fits this definition.
- There are similarities between FOI and EIR for accessing information and it is essential that forces deal with requests under the correct regime.

What Environmental Information do we need to publish?

- The Regulations require you to publish information by easily accessible electronic means and forces should organise their records in such a way that they can publish certain information routinely.
- Forces do not have to publish all the environmental information they hold. The minimum that should routinely be published to comply with obligations under the Regulations provided by this [link](#)³⁶.

What should we do when we receive a request for environmental information?

- Practitioners have to treat enquiries formally as a request under the Regulations. The sensible approach to provide better customer service is to deal with it as a normal customer enquiry under your usual customer service procedures. The legal requirements under EIR may come into force if you cannot provide the requested information straightaway; or the requestor makes it clear they expect a response under the legislation.
- [ICO guidance](#)³⁷ details the handling of requests for information under EIR
- If a request is unclear and 'too general' practitioners can refuse to answer a request (Regulation 12(4)(c)), provided the practitioner has engaged with the requester and asked for extra information, offering them advice and assistance to help to explain, clarify and rephrase their request.
- As with FOI a public authority has 20 working days to go back to the requester for further information. If you do this, you don't have to respond until clarification is provided and you then have 20 working days to respond to the refined request.
- Complex requests can be submitted which makes the timescale more difficult to achieve. In exceptional circumstances only, the Regulations permit public authorities to extend the 20 working day limit to 40 working days to provide more time to answer the request. Applicants must be notified of the extension of time as soon as possible. Failure to respond within a time limit would be a breach of Regulation 5.

What happens if we don't have the information?

Public authorities will not always hold the information requested. Regulation 12(4)(a) stipulates that a formal refusal notice must be issued to the applicant advising them that you do not hold the information.

As with FOI there is no requirement under EIR Regulations for public authorities to create an

³⁶ [What environmental information do we need to publish? | ICO](#)

³⁷ [Guide to the Environmental Information Regulations | ICO](#)

answer in order to respond to a request. That being said, if the applicant has asked a question and your force does not hold recorded information but can answer it, although there is no requirement to do so under the Regulations, it would be considered as good customer service to do so.

If the information isn't held by your force but you know that the information is held by another public authority you should advise the applicant to redirect their request or seek permission to transfer to request to the other public authority.

For more information about good practice in transferring requests for information, see Part VI of the Code of Practice³⁸ on the discharge of the obligations of public authorities under the Environmental Information Regulations 2004.

Do forces have to advise the applicant what information is held?

Forces should always respond in writing to a request and should normally let an applicant know whether or not the requested information is held. The only exclusions to this is detailed under Regulation 12(6) where a public authority does not have to confirm or deny whether the requested information exists and is held, if this would adversely affect the matters listed under regulation 12(5)(a); and confirming or denying that you hold information would contravene the GDPR or the Data Protection Act, Regulation 13(5A) and 13(5B).

In what form or format should the information be provided?

Regulation 6 covers the rights about the form and format of information that has been requested and focuses on what is reasonable. The Regulations go further than the Freedom of Information Act inasmuch as it allows the applicant to specify the form and format of information (the Act only covers form). The form is the way a piece of information is communicated, for example in electronic or hard copy; the format is how the data is arranged within that form, for example using a specific software format.

Can information be changed or deleted that has been requested before providing it?

No. Deletion could be a criminal offence under Regulation 19 if the deletion is intended to prevent disclosure. Information should normally be disclosed that is 'held' at the time a request is made.

Do the Environmental Information Regulations allow us to disclose information to a specific person or group alone?

Disclosures under the Regulations are 'to the world'. However, public authorities can restrict the release of information to a specific individual or group at your discretion, by providing information outside the scope of the Regulations

If a force makes a restricted disclosure, you should make it very clear to the requester that the information is for them alone. However, if the requester has made it clear that they want the information under the regulations, and isn't satisfied with receiving it on a discretionary basis, the information must be provided to the applicant with no restrictions; or forces can refuse the request if an exception applies.

Can we charge for the information?

Yes in some circumstances public authorities can charge a fee for making the information available. Any charge should be 'reasonable' – it should not exceed the costs you incur in making the information available. It may cover the cost of the paper for photocopying or printing the information and a covering letter and the cost of postage. It should not include the cost of staff time in identifying, locating or retrieving the information from storage.

As with Freedom of Information a public authority can charge for environmental information only if you proactively publish a schedule of charges and details of when you may or may not charge. This gives the requester an opportunity to consider the cost of their request before making it.

It is encouraged that public authorities publish this information as part of their Freedom of Information Act publication scheme, keeping the information up to date and in line with your duty under the Regulations to proactively make information available.

DATASET PROVISION

The dataset provisions are not relevant to the Environmental Information Regulations. If a public authority receives a request for an environmental dataset, and the requester has asked for it in a reusable form, the authority should consider its duties under Regulation 6 of the EIR relating to making information available in a particular form or format.

The ICO guidance on dataset provisions advises that the Information Commissioner considers that the term "a particular form or format" in Regulation 6(1) of the EIR can encompass a reusable form. Public authorities should make the environmental dataset available in a reusable form, so far as reasonably practicable.

Under EIR requesters have the right to ask that information be made available to them in a particular form or format when they make their initial request. The form is the way a piece of information is communicated, for example in electronic or hard copy; the format is how the data is arranged within that form, for example using a specific software format.

However, if a public authority cannot put the information into the requested form or format, or the information is already publicly available and easily accessible in another form or format, you don't have to provide the information in the way the requester specifies

APPENDIX 2

MODEL PUBLICATION SCHEME

This model publication scheme has been prepared and approved by the Information Commissioner. It may be adopted without modification by any public authority without further approval and will be valid until further notice.

This publication scheme commits an authority to make information available to the public as part of its normal business activities. The information covered is included in the classes of information mentioned below, where this information is held by the authority. Additional assistance is provided to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner.

The scheme commits an authority:

- To proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the authority and falls within the classifications below.
- To specify the information which is held by the authority and falls within the classifications below.
- To proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within this scheme.
- To produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public.
- To review and update on a regular basis the information the authority makes available under this scheme.
- To produce a schedule of any fees charged for access to information which is made proactively available.
- To make this publication scheme available to the public.
- To publish any dataset held by the authority that has been requested, and any updated versions it holds, unless the authority is satisfied that it is not appropriate to do so; to publish the dataset, where reasonably practicable, in an electronic form that is capable of re-use; and, if any information in the dataset is a relevant copyright work and the public authority is the only owner, to make the information available for re-use under the terms of the Re-use of Public Sector Information Regulations 2015, if they apply, and otherwise under the terms of the Freedom of Information Act section 19. The term 'dataset' is defined in section 11(5) of the Freedom of Information Act. The term 'relevant copyright work' is defined in section 19(8) of that Act.

Classes of information

Who we are and what we do.

Organisational information, locations and contacts, constitutional and legal governance.

What we spend and how we spend it.

Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.

What our priorities are and how we are doing.

Strategy and performance information, plans, assessments, inspections and reviews.

How we make decisions.

Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.

Our policies and procedures.

Current written protocols for delivering our functions and responsibilities.

Lists and registers.

Information held in registers required by law and other lists and registers relating to the functions of the authority.

The services we offer.

Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

The classes of information will not generally include:

- Information the disclosure of which is prevented by law, or exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure.
- Information in draft form.

Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

The method by which information published under this scheme will be made available

The authority will indicate clearly to the public what information is covered by this scheme and how it can be obtained.

Where it is within the capability of a public authority, information will be provided on a website. Where it is impracticable to make information available on a website or when an individual does not wish to access the information by the website, a public authority will indicate how information can be obtained by other means and provide it by those means.

In exceptional circumstances some information may be available only by viewing in person. Where this manner is specified, contact details will be provided. An appointment to view the information will be arranged within a reasonable timescale.

Information will be provided in the language in which it is held or in such other language that is legally required. Where an authority is legally required to translate any information, it will do so. Obligations under disability and discrimination legislation and any other legislation to provide information in other forms and formats will be adhered to when providing information in

accordance with this scheme.

Charges which may be made for information published under this scheme

The purpose of this scheme is to make the maximum amount of information readily available at minimum inconvenience and cost to the public. Charges made by the authority for routinely published material will be justified and transparent and kept to a minimum.

Material which is published and accessed on a website will be provided free of charge.

Charges may be made for information subject to a charging regime specified by Parliament.

Charges may be made for actual disbursements incurred such as:

- photocopying
- postage and packaging
- the costs directly incurred as a result of viewing information

Charges may also be made for information provided under this scheme where they are legally authorised, they are in all the circumstances, including the general principles of the right of access to information held by public authorities, justified and are in accordance with a published schedule or schedules of fees which is readily available to the public.

Charges may also be made for making datasets (or parts of datasets) that are relevant copyright works available for re-use. These charges will be in accordance with the terms of the Re-use of Public Sector Information Regulations 2015, where they apply, or with regulations made under section 11B of the Freedom of Information Act, or with other statutory powers of the public authority.

If a charge is to be made, confirmation of the payment due will be given before the information is provided. Payment may be requested prior to provision of the information.

Written requests

Information held by a public authority that is not published under this scheme can be requested in writing, when its provision will be considered in accordance with the provisions of the Freedom of Information Act.