

Freedom of Information Act Environmental Information Regulations



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

The exemption for personal information

The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) provide rights of public access to information held by public authorities. This is part of a series of guidance notes produced to help public authorities understand their obligations and to promote good practice.

This guidance will explain the interface between freedom of information and the Data Protection Act 1998 (DPA). It will help public authorities to apply the exemption for personal information contained in section 40 of the FOIA, or to apply the equivalent provisions in the EIR.

This guidance replaces Awareness Guidance 1.

Overview

- Section 40 sets out various exemptions from the right to know for information that is personal data protected by the DPA. Most of these exemptions are absolute, which means there is no additional public interest test.
- Personal data is defined in the DPA and will include any recorded information in any form relating to an identifiable living person.
- Personal data of the applicant is exempt under section 40(1) of the FOIA. These requests should instead be dealt with as DPA subject access requests.
- Personal data of any other person (third party data) is exempt under section 40(2) if disclosure would breach one of the data protection principles. Generally this will mean considering whether it is unfair to release the information and balancing the necessary public interest in disclosure against the interests of the individual under the first principle.
- There are also exemptions for third party data if formal objections have been made or if subject access exemptions apply, but these are rarely used. These exemptions are qualified, which means they are subject to a public interest test.
- The EIR contain similar provisions. Personal data of the applicant is exempt under regulation 5(3) of the EIR. The exception for third party data is set out in regulations 12(3) and 13(1).

General principles of exemption

Section 40 of the FOIA sets out an exemption from the right to know if the information requested is personal information protected by the DPA. The section has a fairly complex structure and refers in detail to DPA provisions and concepts.

Equivalent exceptions are set out in regulations 5(3), 12(3) and 13 of the EIR. This guidance is also relevant to these regulations, which should be applied in exactly the same way as section 40. However, for ease of reference the specific EIR regulation numbers are set out separately on page 11.

The exemption is designed to address the tension between public access to official information and the need to protect personal information. Freedom of information requires the release of publicly held non-exempt information, and wrongly withholding information will breach the FOIA. However, wrongly releasing an individual's personal information will breach the DPA. It is therefore very important to understand and apply this exemption correctly to ensure compliance with both regimes.

The exemption is an absolute exemption (except in some limited circumstances). This means that if the information falls within the exemption, there is no need to consider an additional public interest test.

However, information is not automatically exempt just because it is personal data. You will need to consider the details of the exemption. Any refusal notice will need to explain exactly which subsection applies, and why.

Section 40(1) sets out the exemption if the applicant is requesting their own personal data. These requests should be considered instead as subject access requests under section 7 of the DPA.

Section 40(2) sets out the exemption for someone else's personal data (third party data) if one of the conditions in section 40(3) or 40(4) is met. These conditions require you to refer back to the DPA. The most common condition for the exemption to apply is where disclosure would breach one of the data protection principles contained in Schedule 1 of the DPA. You will therefore generally need to start with two broad questions:

- Is the information "personal data"?
- If so, will disclosure breach one of the data protection principles?

Duty to confirm or deny

You should also remember your duty to confirm or deny whether you hold the information. Even if the information itself is exempt from disclosure, you may still need to confirm that you hold it unless the confirmation itself would be exempt under section 40(5). Equally, if you do not hold the information, you must say this unless the denial itself would be exempt. For further information

on the duty to confirm or deny, see [The duty to confirm or deny: Awareness Guidance 21](#).

Is the information personal data?

The first step is to determine whether the requested information is (or contains) personal data. Section 40(7) of the FOIA confirms that the relevant definition is set out in section 1(1) of the DPA:

“personal data” means data which relate to a living individual who can be identified—

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The information itself can be in any form, including electronic data, images, and paper files or documents. It does not have to be held in a database or filing system to be caught and will include so-called “category (e) data” – recorded information held in a manual, ‘unstructured’ form by a public authority. Essentially any reference to an individual in any document or other information held by a public authority can be personal data.

Whether information is personal data will often be obvious. The two main elements of personal data are that the information must “relate to” a living person, and that person must be identifiable. Information will “relate to” a person if it is about them, linked to them, has some biographical significance for them, is used to inform decisions affecting them, has them as its main focus or impacts on them in any way.

For more information on what amounts to personal data, see our DPA technical guidance notes: [Determining what is personal data](#) and [What is personal data? - A quick reference guide](#).

Applicant’s own personal data

If the requested information is the applicant’s own personal data, there is an absolute exemption from FOIA access rights under section 40(1). In addition, section 40(5)(a) provides an exemption from the duty to confirm or deny.

Instead, the request will be a DPA subject access request and you will need to deal with it in accordance with the DPA. You must comply with the subject access request promptly and in any event within 40 calendar days. Strictly speaking, however, the FOIA time limits still apply, and although the information is exempt you are technically required to issue a refusal notice. For practical purposes, we therefore advise that public authorities respond to subject access

requests within 20 working days or else explain within this time limit that the request is being dealt with under the DPA.

For more information on how to deal with subject access requests, see our DPA guidance: [Checklist for handling requests for personal information \(subject access requests\)](#).

If the requested information is the applicant's own personal data but also includes information about other people, you should still deal with it as a subject access request. Section 40(1) of the FOIA still applies and you should handle the third party data in accordance with the relevant subject access provisions under the DPA. For more information, see our DPA guidance: [Dealing with subject access requests involving other people's information](#).

You should only use section 40(1) and deal with a request as a subject access request if the identity of requester is clear and you can confirm that the information is their personal data. You can ask for proof of identity, but as the FOIA is generally applicant-blind you should not insist. If you have any doubt about the identity of the applicant, you must deal with the request as a request for third party data.

Someone else's personal data

If the requested information is (or contains) other people's personal data, section 40(2) may apply. Section 40(2) sets out an exemption for third party data if one of the four conditions set out in section 40(3) or 40(4) is met.

The usual situation where the exemption will apply – and the focus of this guidance – is where disclosure of the personal data would breach one of the data protection principles set out in schedule 1 of the DPA. This is an absolute exemption, which means that if the condition is satisfied there is no additional public interest test to consider.

There are also two qualified exemptions, which are subject to the public interest test. These are discussed further on page 10, but are rarely used.

You may however still need to confirm or deny whether you hold the information, even if the information itself is exempt. Section 40(5)(b)(i) provides that the duty to confirm or deny still arises unless the confirmation or denial itself would breach the data protection principles or section 10 of the DPA (data subject's right to prevent processing), or is exempt from section 7(1)(a) DPA (data subject's right to be informed whether personal data is being processed).

- **Breach of the data protection principles**

Section 40(2) together with the condition in section 40(3)(a)(i) or 40(3)(b) provides an absolute exemption if disclosure of the personal data would breach any of the data protection principles.

The exemption will apply to all forms of recorded information, even manual category (e) data. Even though the data protection principles do not fully apply to category (e) data (see section 33A of the DPA), the condition in section 40(3)(b) confirms that the disclosure should be considered as if the principles did apply.

There are eight data protection principles. However, for the purposes of disclosure under the FOIA, it is only the first principle – that data should be processed fairly and lawfully – that is likely to be relevant.

The second principle states that “personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes”. We consider that a FOIA disclosure that complies with the DPA in other respects will not breach the second principle.

The third, fourth and fifth principles are likely only to be relevant to holding and using data, not to disclosure. The sixth principle requires that data be processed in accordance with the rights of individuals under the DPA, and is unlikely to add anything to the first principle in the context of disclosure under the FOIA. The seventh principle relates to the accidental loss or abuse of data. Finally, the eighth principle concerns adequate protection when transferring data outside the EEA. Again, consideration of these principles is unlikely to add anything where it is fair to release the information to the public at large under the first principle.

The key question will therefore be: is it fair and lawful to release the information under the first principle?

- **The first data protection principle**

The first data protection principle states:

- 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—*
 - (a) at least one of the conditions in Schedule 2 is met, and*
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.*

Disclosure must therefore be fair, lawful and meet one of the relevant DPA Schedule conditions. In the context of the FOIA, we recommend that you consider whether disclosure satisfies one of the specific conditions first, before moving on to the general consideration of fairness and lawfulness.

There are six conditions in Schedule 2, but only condition 1 (consent) or condition 6 (legitimate interests) should be relevant to disclosure under the FOIA. The other conditions all refer to disclosure for a specific purpose, which cannot apply as the FOIA is applicant- and motive-blind: you are disclosing to the public at large and cannot take the identity, intentions or purpose of the

applicant into account. You should also note that the FOIA itself cannot be used to meet the third condition (that disclosure is necessary for compliance with a legal obligation). Section 40(3) of the FOIA makes clear that disclosure “otherwise than under this Act” must not breach the principles, which means that you cannot circumvent the requirements of the DPA in this way.

Unless all individuals whose personal data falls within the scope of the request have consented to the release of their information, you will need to consider Schedule 2 condition 6.

- **Schedule 2 condition 6**

Condition 6 requires that:

6.—(1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

As disclosure under the FOIA is considered disclosure to the public at large and not to the individual applicant, you will therefore need to balance the legitimate public interest in disclosure against the interests of the individual whose data it is. Although this requires consideration of the public interest in disclosure, the test is not the same as the public interest test used for qualified exemptions and there is no assumption of disclosure.

Following the Tribunal decision in [Corporate Officer of the House of Commons v Information Commissioner and Leapman, Brooke and Thomas \(EA/2007/0060 etc; 26 February 2008\)](#) (upheld on appeal by the High Court¹), we recommend that public authorities approach condition 6 as a three-part test:

1. there must be a legitimate public interest in disclosure;
2. the disclosure must be necessary to meet that public interest; and
3. the disclosure must not cause unwarranted harm to the interests of the individual.

Firstly, you should identify any legitimate public interest in disclosure. There must be genuine public interest at stake, not mere public curiosity. There is always some public interest in the principle of freedom of information and this will be one relevant factor to consider, but you should also consider the particular circumstances of the case.

¹ [Corporate Officer of the House of Commons v Information Commissioner and Brooke, Leapman and Ungood-Thomas](#) [2008] EWHC 1084 (Admin)

Relevant considerations could include arguments relating to transparency, accountability, the number of people affected by a decision or how public money is being spent.

For example:

The [Leapman, Brooke and Thomas](#) case concerned disclosure of details of some MPs' expenses. The Tribunal considered that there were clear legitimate public interests at stake, related to the objectives of transparency, accountability, value for money and the health of our democracy. Specifically, those interests included the general principle of FOI, public scrutiny of the use of public funds, encouraging MPs to make better value for money choices, assessing politicians' probity, enhancing public confidence in parliament, and informing public debate on reforms of the allowance system. The legitimacy of these interests was enhanced by a history of mistakes and misuse of the expenses system, and the fact that MPs themselves certified the system without independent oversight.

You will then need to assess whether disclosure is necessary to achieve each of these aims, or whether there is another way to address the public interest that would interfere less with the privacy of individuals. Can any other existing mechanisms achieve the same result without the disclosure? Factors to consider could include a current lack of transparency and absence of other effective controls – for example, because a directly elected official is accountable mainly to the public, or because a system is self-certified without independent oversight – or a long history of controversy, which could suggest that other means have proved ineffective.

For example:

In [Leapman, Brooke and Thomas](#), only full disclosure could address the serious inadequacies of the expenses system and the longstanding lack of public confidence in it. A stated intention to reform that system in future was irrelevant. In addition, the status of MPs as elected representatives with accountability at the ballot box was only meaningful if voters had sufficient details to make a properly informed decision when voting.

Finally, even if the disclosure is necessary to meet a legitimate public interest, you will need to weigh up whether that disclosure would nevertheless be an unwarranted interference with the individual's privacy. Essentially, this stage involves balancing the interests of the individual against the public interest in disclosure you have identified – ie against the collective weight of the public interest factors that have passed the necessity test. Factors to consider when weighing the interests of the individual may include:

- Whether the information relates to the individual's public life (ie their work as a public official or employee) or their private life (ie their home, family, social life or finances). Information about an individual's private life will deserve more protection than information about them acting in an official or work capacity. You should also consider the seniority of their position, and whether they have a public-facing role. The more senior a person is, the less likely it is that disclosing information about their public duties will be unwarranted or unfair. Information about a senior official's public life should generally be disclosed unless it would put them at risk, or unless it also reveals details of the private lives of other people (eg the official's family).
- The potential harm or distress that may be caused by the disclosure. For example, there may be particular distress caused by the release of private information about family life. Some disclosures could also risk the fraudulent use of the disclosed information (eg details of bank accounts) or pose a security risk (eg addresses, work locations or travel plans where there is a risk of harassment or other credible threat to the individual), which is unlikely to be warranted. However, the focus should be on harm or distress in a personal capacity. A risk of embarrassment or public criticism over administrative decisions, or the interests of the public authority itself rather than the individual concerned, should not be taken into account.
- Whether the individual has objected to the disclosure. However, although such an objection would be a relevant factor, it is not automatically enough to make the disclosure unwarranted or unfair. You must consider all the circumstances of the case.
- The reasonable expectations of the individual as to whether their information would be disclosed. However, in the absence of other factors disclosure will not be automatically unwarranted or unfair just because the person was not aware of the possibility of disclosure. It is not possible to avoid your duties under the FOIA by not telling individuals that their data may be disclosed, or by stating that data will not be disclosed, and then arguing that disclosure would be unwarranted and unfair.

Disclosure will always involve some intrusion with privacy, but that intrusion will not always be unwarranted. You must consider all the circumstances of each case.

For example:

In [Leapman, Brooke and Thomas](#), the Tribunal considered that disclosure of details of MPs' second home expenses would not be unwarranted. MPs should expect a greater degree of scrutiny, and information related to expenses was incurred as a result of their public duties even though it included some information about their home life. The potential for public misunderstanding about the disclosed information was not a compelling argument.

On the other hand, disclosure of information on other people's private lives (eg partners and children) was unwarranted, as was disclosure of bank account details due to the risk of fraud, and details of contractors with access to the house or full addresses where there was a known security threat against the MP.

If you think that full disclosure is unnecessary or would cause an unwarranted interference, you should consider whether disclosure of part of the information would be possible instead.

If disclosure does not meet this condition, the information cannot be disclosed and there is no need to go on to the general consideration of fairness and lawfulness.

- **Is disclosure otherwise fair and lawful?**

In addition to meeting a Schedule 2 condition, to comply with the first principle any disclosure must also be fair and lawful.

This requires a more general consideration of fairness. For practical purposes, disclosure will generally be fair if Schedule 2 condition 6 has been satisfied. This is because a general consideration of fairness will involve balancing very similar issues to those set out above.

If you have the data subject's consent to the disclosure under Schedule 2 condition 1 and have therefore not already considered condition 6, you will now need to consider whether the disclosure would be fair. It is likely that disclosure with consent will usually be fair, but you should take care to look at all the circumstances, particularly if consent was not explicit or where the individual concerned is young or otherwise vulnerable.

Disclosure under the FOIA will usually be lawful, unless there is a specific law forbidding disclosure. However, in those cases another exemption will generally be easier to apply: for example, section 44 (for any statutory prohibitions) or section 41 (for a breach of confidentiality).

We consider that the Human Rights Act 1998 will not make any fair disclosure unlawful, as the right to privacy will have been fully taken into account when considering the balance of fairness and the Schedule 2 conditions.

- **Sensitive personal data**

If the information is sensitive personal data, the proposed disclosure will need to satisfy a condition in Schedule 3 of the DPA as well as in Schedule 2. Sensitive personal data is defined in section 2 of the DPA and includes information relating to an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life
- criminal offences, sentences, proceedings or allegations

If the information falls into one of these categories, you should consider Schedule 3 first. This is because if none of the Schedule 3 conditions apply, the information cannot be disclosed and there is no need to go on to consider Schedule 2 or the general balance of fairness.

It is unlikely that you will be able to satisfy any of the Schedule 3 conditions unless you have explicit consent for the disclosure (condition 1), or the information has already been made public by the individual concerned (condition 5) – for example, the political affiliations of MPs. This is because the other conditions concern disclosure for a stated purpose, and therefore cannot be relevant to the applicant- and purpose-blind nature of disclosure under the FOIA.

It is therefore very unlikely that sensitive personal data could be released in response to an FOI request without explicit consent.

- **Qualified exemptions**

Section 40(2) also contains two alternative exemptions for third party data. However, for practical purposes it is hard to think of a situation when these might be useful, as it is highly likely that the main third party data exemption or other FOIA exemptions will be easier to apply.

Section 40(2) together with the condition in section 40(3)(a)(ii) provides a qualified exemption if disclosure would breach section 10 of the DPA. This applies where the public authority has already agreed not to process the relevant personal data due to a formal notice from the individual concerned (a data subject notice) that it would cause unwarranted damage or distress to them. However, in such cases it is likely that the disclosure would be unfair and therefore the main s40(2) exemption would also apply.

Section 40(2) together with the condition in section 40(4) provides a qualified exemption where the information would be exempt under the DPA from a subject access request. The relevant provisions are set out in Part IV of the DPA and examples include information protected by legal professional privilege,

or information used in the prevention and detection of crime. However, in such cases it will usually be easier to apply the equivalent FOIA exemption.

As these exemptions are qualified, even if information falls within one of the exemptions you must go on to apply the public interest test set out in section 2(2)(b) of the FOIA. The information can only be withheld if the public interest in maintaining the exemption outweighs the public interest in disclosure.

Environmental information

If the information being considered is environmental information, disclosure must be considered under the provisions of the EIR rather than the FOIA. For more information on what constitutes environmental information, see our guidance: [What is environmental information?](#)

The structure and wording of the EIR provisions on personal information mirror section 40 and can be used in exactly the same way. The relevant regulations are as follows:

- **Definitions**

Regulation 2(4) confirms that you should refer to the definition of personal data and the data protection principles set out in the DPA.

- **Applicant's own personal data**

Regulation 5(3) states that the duty to make environmental information available on request does not apply to personal data of the applicant. This will also mean that there is no need to confirm or deny that you hold the information or to issue a refusal notice. These requests should instead be dealt with as subject access requests.

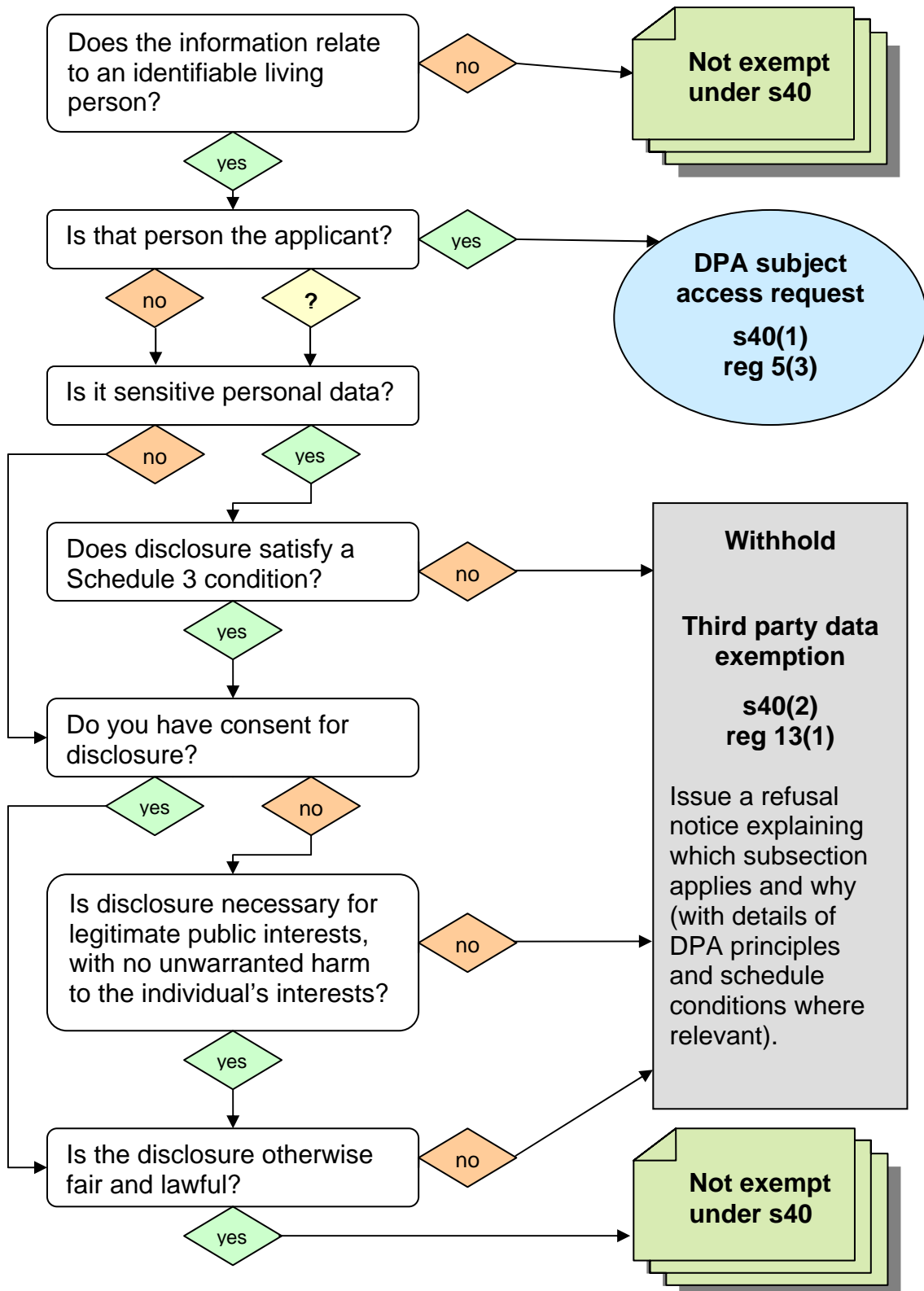
- **Someone else's personal data**

Regulation 12(3) provides that third party data can only be disclosed in accordance with regulation 13, which sets out the detail of the exception.

The main exception for disclosure that would breach the data protection principles is set out in regulation 13(1) together with the condition in 13(2)(a)(i) or 13(2)(b). There is no additional public interest test. Regulation 13(5)(a) provides that you can refuse to confirm or deny that you hold information if the confirmation (or denial) would itself breach the data protection principles.

The qualified exceptions are contained in regulation 13(1) taken with the condition in 13(2)(a)(ii) if disclosure would breach section 10 of the DPA, or 13(3) if the information would be exempt from subject access requests.

Summary of approach



Other considerations

Many freedom of information requests will include information about public authority employees. You should ensure that you have a clear policy so that

staff know what sort of information they should expect to be routinely disclosed, and what might legitimately be withheld. It may also be helpful to have a similar policy for any other individuals about whom you hold significant information (eg patients, pupils, residents etc).

Additional guidance is also available from our website if you need further information on:

- Any aspect of the Data Protection Act 1998
⇒ see www.ico.gov.uk/what_we_cover/data_protection/guidance.aspx
- Requests for information about your staff
⇒ see [Access to information about public authorities' employees](#)
- Requests for information containing an individual's name
⇒ see [When should names be disclosed?](#)
- Requests for complaints and investigations files
⇒ see [Complaints and investigations files – how to approach them](#)
- Requests for information about deceased individuals
⇒ see [Information about the deceased](#)

More information

This guidance will be reviewed from time to time in line with new decisions of the Information Commissioner, Tribunal and courts on freedom of information cases. It is a guide to our general recommended approach to this area, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of freedom of information, please contact us.

Phone: 08456 30 60 60
01625 54 57 45

Email: please use the online [enquiry form](#) on our website

Website: www.ico.gov.uk