FOI Exemptions: Personal Information

Section 40 of the Freedom of Information Act 2000 exempts personal data from disclosure. If the request is for the requester's own data, the exemption is absolute and the request belongs on the subject access route. If the data is about someone else, it applies only where disclosure would breach the data protection principles, or one of two further conditions is met. Only the first of those conditions is absolute.

AT A GLANCE

Section	Section 40 FOIA. Section 38 FOISA in Scotland. Regulation 13 for environmental information
Type	Section 40(1) is absolute. Section 40(2) is absolute where the first condition is met, and qualified for the second and third conditions
Main test	Would disclosure to the public breach the data protection principles, most often lawfulness, fairness and transparency
Neither confirm nor deny	Available under section 40(5A) and 40(5B)
Refusal notice	Name section 40 and the condition you rely on, and explain why it applies

1. What counts as personal data in an FOI request?

Personal data is information that relates to an identified or identifiable living person. A name is the obvious case, but a job title, a small team, an email address or a combination of details can identify someone just as well. If a requester could work out who is meant, treat it as personal data.

Information about people who have died is not personal data under data protection law. It may still be protected by another exemption, such as confidence. For a fuller explanation, see our guide, What Is Personal Data? A Guide for DSAR Teams.

2. When is an FOI request really a subject access request?

Where the information requested is the requester's own personal data, section 40(1) exempts it, and section 40(5A) means you need not confirm whether you hold it. There is no public interest test. The request is not refused and forgotten. You should recognise that the person is entitled to ask for their own data under the right of access, and handle it as a subject access request under the one month deadline.

Mixed requests are common. A person asks for a policy document and for the notes about their own complaint. Split the request, answer the policy part under FOI and route the rest to the DSAR process. Our DSAR process hub shows where that fits.

3. How do you decide whether disclosing someone else's data breaches the principles?

For information about other people, the first condition in section 40(3A) asks whether disclosure to a member of the public, outside the Act, would contravene the data protection principles. In practice the question is nearly always lawfulness, fairness and transparency, and the lawful basis most often considered is legitimate interests. Work through three questions in order.

1. **Is there a legitimate interest?** Accountability for public money, transparency about decisions and understanding how a service works can all qualify. The requester's interest, or the public's wider interest, both count.
2. **Is disclosure necessary?** Could the legitimate interest be met by something less intrusive, such as anonymised or aggregated information? If so, disclosure of the personal data is not necessary.
3. **Do the person's interests override it?** Consider their reasonable expectations, the harm disclosure could cause, and their role. People in senior or public facing roles should expect more scrutiny than junior staff, and information about their working lives carries different weight from information about their private lives.

If the answer to the first condition is yes, the exemption is absolute and there is no further public interest test. Keep the written reasoning, because it is what an internal review and the regulator will test.

4. What are the second and third conditions?

The second condition applies where disclosure would contravene the right to object in Article 21 UK GDPR. The third applies where the information would be withheld if the person asked for it under the right of access, because of an exemption in the Data Protection Act 2018. Both are qualified. You must weigh the public interest in disclosure against the public interest in withholding, and give reasons.

Do not skip this step because the information is clearly personal. A qualified exemption with a considered public interest assessment is stronger than an assumption.

5. Do you have to confirm or deny that you hold the information?

Not always. Section 40(5B) removes the duty to confirm or deny where doing so would itself disclose personal data, for example confirming that a named employee is under disciplinary investigation. If you use it, apply it consistently, so that your response to a request about someone who is not under investigation reads the same as one about someone who is. Otherwise the pattern gives the answer away.

WORKED EXAMPLE (ILLUSTRATIVE)

A council receives a request for the names and work email addresses of everyone in its housing department, and for the outcome of a complaint made about one named officer.

- **Names and emails of senior and public facing staff.** There is a legitimate interest in knowing who is accountable. Disclosure is necessary to meet it, and these staff would reasonably expect to be identified. Disclose.
- **Names of junior staff with no public role.** The interest can be met by publishing job titles and the team structure. Withhold the names under section 40(2), first condition.
- **The complaint outcome about the named officer.** The council applies section 40(5B) and neither confirms nor denies whether it holds the information, because confirming would disclose that a complaint about that person exists.

The case record notes each decision, the condition relied on and the reasoning. That record is the evidence if the requester asks for an internal review.

6. Tracking personal data decisions: spreadsheet or structured case workflow

Task	Spreadsheet and email	Structured case workflow
Spotting a mixed FOI and subject access request	Found when someone reads the whole request	Request type recorded, with the ability to split a multi part request into separately managed cases
Recording the exemption and reasoning	A note in the margin or an email thread	Exemption and reason recorded against the case and added to the audit log
Meeting the 20 working day deadline	Bank holidays counted by hand	Deadline tracking that accounts for bank holidays
Evidence at internal review	Rebuilt from emails	Timeline and audit log already attached to the case

Frequently asked questions

Is the name of a council officer always exempt?

No. It depends on their role, seniority and what the name is attached to. Apply the three questions each time, and do not use a blanket rule.

Can we refuse because the requester gave a name and we cannot verify them?

Not under section 40. Identity matters for subject access requests. An FOI response is a disclosure to the world, so the question is whether it is acceptable for anyone to see the information.

Is section 40 subject to the public interest test?

Section 40(1) and the first condition in section 40(2) are absolute. The second and third conditions are qualified, so the test applies.

What if the individual consents?

Consent is relevant to fairness and lawfulness, but it must be freely given and specific. Without it, rely on the legitimate interests assessment.

THE PITFALL

Applying a blanket rule that every staff name is exempt, or that every name is disclosed.

THE REMEDY

Work through legitimate interest, necessity and the person's interests for each name, and record the answer.

KEY TAKEAWAYS

- Own data goes to the subject access route. Do not simply refuse.
- For third party data, the first condition is absolute and the other two are qualified.
- Work through legitimate interest, necessity and the person's interests, and write down the answer.
- Senior and public facing roles carry less expectation of privacy than junior ones.
- Use neither confirm nor deny where confirmation would itself disclose personal data, and apply it consistently.

Conclusion: prioritise the right route, a written test and consistent responses

If your team is small and the deadline is close, start by sorting own data requests from third party data. Then run the same three questions on every name, and write the answer down as you go.

HOW PROVEPRIVACY HELPS

ProvePrivacy DSAR & FOI (Lite) manages FOI, EIR, FOI (Scotland), EIR (Scotland) and CHAIRs (Housing) requests in one case workflow, alongside data subject rights requests. Fee and public interest delay management is built in, and the Disclosure tab records the exemptions relied on and the reason for each, adding them to the case audit log. The same platform handles the subject access side, so a mixed request does not leave your team working in two places.

Where this fits in the FOI process

Section 40 is applied at the decision stage of the request, after you have found the information and before you respond. See our FOI process hub for the full journey from receipt to internal review.

SCOTLAND AND ENVIRONMENTAL INFORMATION

Scottish public authorities apply section 38 of the Freedom of Information (Scotland) Act 2002, which follows a similar structure. Environmental information is handled under regulation 13 of the Environmental Information Regulations 2004, where the same conditions apply but every exception is subject to the public interest test. See our guides on EIR exceptions and on FOISA and the EIRs in Scotland.

Related guides

- DSAR Exemptions: Protecting Third Parties
- FOI Exemptions: Legal Privilege and Confidence
- FOI Exemptions: Commercial Interests

Sources

- Freedom of Information Act 2000, sections 2, 10, 17 and 40 (legislation.gov.uk)
- Data Protection Act 2018 and UK GDPR, Articles 5, 6 and 21
- ICO guidance: Personal information (section 40 and regulation 13)
- Scottish Information Commissioner guidance: Personal information (section 38)

Talk to someone who has handled FOI

Book a demo, request a quote or arrange a 15 minute call.

www.proveprivacy.com | hello@proveprivacy.com