Disclosure of ICO employee information policy

Version number: 1.0

Status: Published

Department/Team: Information Access Team

Relevant policies: Staff Privacy Notice, Data Protection Policy, Personal data sharing policy

Distribution: Internal and external.

Author/Owner: [redacted] Information Access

Consultees: Various

Approved by: Louise Byers

Application date: 16/02/2026

Review date: 16/02/2027

Security classification: Official

Key messages

The main objective of this policy is to provide:

- Clarity on what information you might reasonably expect to be routinely disclosed about you by the ICO.
- This includes disclosures into the public domain under the provisions of the Freedom of Information Act 2000 (FOIA), including information we proactively disclose as part of our publication scheme.
- It also addresses what information may be disclosed about you in responses to individual information rights requests and any other legal obligations we may have.

Does this policy relate to me?

This policy applies to:

- Full-time and part-time employees (both present and former)
- Temporary employees and agency staff
- Secondees, consultants and apprenticeships
- Non-Executive Directors
- Visiting researchers and external speakers

Table of Contents

1. Introduction

1.1. The Information Commissioner's Office is committed to the principles of openness and transparency, recognising that these values are essential to enhancing public accountability. We follow the ICO's model publication scheme and in particular, the definition document for non-departmental public bodies in order to comply with our duties under section 19 of the FOIA. More information can be found on our publication scheme compliance page. It includes information we proactively publish, including about our Management board and decision making structure, as well as our register of interests. Examples of details other public authorities routinely publish, including details such as the names,

job titles, and salaries of senior civil servants can be found on the government's Find Open Data website.

1.2. This policy outlines our approach to disclosing employee information and what staff can reasonably expect us to disclose about them. It provides guidance for staff and request handlers on disclosures under FOI, data protection legislation, and what we proactively publish, and should be read with our staff privacy notice. While not exhaustive, it explains our general approach to handling such information.

1.3. We generally disclose employee information only as outlined in this policy and the staff privacy notice. While we would not typically consult with individuals prior to disclosure, we may do so where the information in question is not reasonably expected to be shared. In such instances, we will ensure that any disclosure is appropriately justified, compliant with data protection legislation, and consistent with our internal policies.

1.4. This policy is not intended to cover the disclosure of ICO staff information where it can be disclosed in an anonymised or aggregated format. In such cases we will establish that ICO staff are not identifiable prior to making a decision on disclosure.

1.5. Information relating to deceased individuals is no longer considered to be personal data. However, other exemptions may apply and disclosure will be considered on a case by case basis.

1.6. If there are exceptional circumstances where the release of your identity would result in harm to you or others close to you, please contact HR and the Information Access Team. Further details on how to do so can be found in part 5 of this policy.

Back to the top

2. Disclosures under FOIA

2.1. As a public authority we regularly receive information requests under the FOIA. This includes requests for the disclosure of information about our employees. This could include, but is not limited to:

- salaries and bonuses;
- information about termination of employment and compromise agreements;
- lists and directories of staff;
- names in documents;
- registers of interests;
- disciplinary files; and
- representatives of other organisations

2.2. Where a request involves personal data of our employees, we must assess whether disclosure would contravene the UK GDPR data protection principles - particularly principle (a), which requires processing to be lawful, fair, and transparent.

2.3. For the purpose of responding to an FOI or EIR request, the relevant processing activity we are undertaking is set out in section 3(4)(d) of the DPA18. That is, "disclosure by transmission, dissemination or otherwise making available".

2.4. In order for the disclosure to be lawful, it must satisfy a lawful basis under Article 6 of the UK GDPR. In most cases, the "legitimate interests" basis (Article 6(1)(f)) is the most applicable. If the data includes special category information, an Article 9 condition must also be met. Where the data relates to criminal convictions or offences, including alleged offences and related proceedings, the requirements of Article 10 must be satisfied.

2.5. In order to assess whether we can rely on legitimate interests as our lawful basis, we must consider three key questions:

(i) Legitimate interest test: are you, or the third party seeking access to the information, pursuing a legitimate interest?

(ii) Necessity test: is disclosure necessary to meet those interests?

(iii) Balancing test: do the legitimate interests outweigh the interests and rights of the individual?

2.6. As part of the 'balancing test', we must consider several key issues, including the potential harm or distress disclosure may cause and the reasonable expectations individual ICO employees may have concerning disclosure of their personal data. Details on how we consider these matters can be found in our guidance on Requests for personal data about public authority employees.

2.7. Each request is considered on a case-by-case basis, and we will take in account the employee's role, seniority, location, and any relevant publicly available information (including any information placed into the public domain by employees themselves). Our approach is informed by our guidance, decision notices and Tribunal decisions.

2.8. We will generally disclose more information about staff members who are the equivalent to posts at Senior Civil Service, ie grade G2 (Directors) and above at the ICO.

2.9. This is because these positions are ultimately accountable for decision making about policy and expenditure. Our guidance also states that public figures must expect a degree of scrutiny about their functions in office.

2.10. Decisions will be made on a case by case basis when considering the disclosure of information relating to consultants, visiting researchers and external speakers. We may also consider the application of exemptions other than section 40, such as section 43 (commercial interests) and section 41 (confidentiality).

2.11. The table below illustrates the types of information we would usually disclose about staff. Please note that this table is intended as a general guide only. As explained above, we assess all disclosures on a case by case basis. Decisions on disclosure may depart from the guidelines below where our legitimate interests assessment falls in favour of disclosure.

Type of Information	Grade G2 and Above	Grade G and Below
Names, job titles, work email addresses and work telephone numbers.	Names and job titles likely to be disclosed. Contact details likely to be withheld.	Job titles in most circumstances are likely to be disclosed. Names and contact details are likely to be withheld.
Information regularly contained in staff email signature blocks, such as working patterns and membership of ICO Staff Networks.	Likely to be withheld.	Likely to be withheld.
Salary information.	Individual salary information likely to be disclosed in £5k bands. This is usually a routine disclosure in line with the ICO's publication scheme guidance. Exact salaries are likely to be withheld, in line with our guidance on requests for personal data about public authority employees.	Salary scales for specified job roles and/or grades likely to be disclosed. Exact salaries likely to be withheld.
Other work related information such as: years in post, previous positions held at the ICO etc.	Likely to be disclosed.	Likely to be withheld.
Position in corporate structure, roles, duties, work-related responsibilities	Likely to be disclosed.	Job specifications and job descriptions likely to be disclosed. Organisational

		organogram likely to be disclosed, but no individual staff names disclosed.
Expenses claims	Summaries of expenses claims and amounts claimed by named employees are routinely published and can be found on our Income and expenditure page.	Summaries of expenses claims and amounts claimed, by job title likely to be disclosed, unless this renders an individual identifiable.
Vocational training or secondments undertaken whilst employed at the ICO.	Likely to be disclosed	Likely to be withheld in relation to identifiable individuals.
Business related entries in office diaries or schedules.	Likely to be disclosed, unless any other exemptions apply.	Likely to be withheld in relation to identifiable individuals.
Work-related opinions attributable to an individual, for instance case notes containing opinions about an investigation, or complainant. This includes information held on any corporate systems, including in chat/channel messages exchanged on platforms such as Microsoft Teams, as	Likely to be disclosed, unless there are concerns which would engage other exemptions that may apply.	Likely to be disclosed where we can do so without identifying individual staff members, unless other exemptions are engaged.

well as other tools we use such as Miro.		
Prompts provided to generative AI tools and services (for example, Microsoft Copilot) when used in an official capacity and attributable to an individual.	Likely to be disclosed, unless other exemptions are engaged.	Likely to be disclosed where we can do so without identifying individual staff members, unless other exemptions are engaged.
Personal details obtained by Human Resources as part of the recruitment process, eg: CVs, the content of job application forms, references, qualifications, work histories. Also includes individual appointment letters and contracts.	Likely to be withheld.	Likely to be withheld.
Home addresses / contact details, next of kin information, personal interests and other non work-related information	Likely to be withheld.	Likely to be withheld.
Special category data (for example: trade union membership, ethnicity or sexual orientation).	Likely to be withheld. Aggregated/ anonymised data is disclosed to comply with equality and diversity and Trade union facility time requirements.	Likely to be withheld. Aggregated/ anonymised data is disclosed to comply with equality and diversity and Trade union facility time requirements.

Security clearance information, in particular where, as part of the security clearance process, there is a requirement not to disclose someone's clearance status	Likely to be withheld. Neither confirm nor deny (NCND) provisions are likely to apply.	Likely to be withheld. Neither confirm nor deny (NCND) provisions are likely to apply.
Private entries in office diaries or schedules, e.g., medical personal appointments	Likely to be withheld.	Likely to be withheld.
Details of personal development reviews and other staff interviews, for example, dispute resolution or disciplinary proceedings	Likely to be withheld. NCND provisions are likely to apply to information relating to disciplinary, grievance or other similar processes.	Likely to be withheld. NCND provisions are likely to apply to information relating to disciplinary, grievance or other similar processes.
Sponsorship, membership, and time spent on staff networks and activities	Case by case basis – special category data considerations may apply.	Likely to be withheld.

2.12. The table above is not exhaustive. All FOI disclosures are reviewed individually by the Information Access team, using the principles in this policy, our published guidance and where relevant, the views and circumstances of individual employees.

2.13. The Information Access team will usually only consult with individual staff if disclosure appears to be outside the expectations set out in this policy.

2.14. If we find that disclosure would not contravene the data protection principles, we will go to consider whether we have

received a valid objection to processing under article 21 of the UK GDPR prior to receipt of a request.

2.15. The exemption at section 40(3B) of FOIA sets out that we must not disclose personal information if it would contravene a valid objection to the processing of personal data. However, where this condition is met, the decision on disclosure is subject to the public interest test. More information about your right to object can be found in section 5 of this policy.

2.16. Your personal data may be shared with the Information Access Team in order for it to be considered for disclosure in response to information requests.

2.17. It may also be necessary to keep a copy of the requested information for a specified period (in line with our retention and disposal schedule) in the event it needs to be considered as part of an internal review, complaint to the ICO (as regulator), or Tribunal proceedings. This remains the case even where it is information that would not usually be disclosed in line with this policy.

2.18. Where this information cannot be anonymised, concerns specific individuals and is sensitive in nature, it will usually be processed in the Information Access Team 'restricted access' area of EDRM.

2.19. When dealing with requests for statistical information about ICO staff, the fact that the requested information is about a small number of people does not necessarily preclude it from disclosure. We must ascertain whether an individual can be identified with a degree of certainty before making a decision on disclosure.

2.20. This consideration will include assessing if there is any additional available information which could be combined with the requested information to enable identification and all the means likely to be used to achieve re-identification, including the technology available at the time of the request, for instance generative AI chatbots. Further information can be found in our guidance on the exemption at section 40 of the FOIA: Is the request for personal data?

2.21. If you have any particular concerns or objections to disclosure of your personal data, further details on how to raise such matters can be found in section 5 of the policy.

Back to the top

3. Disclosures in individual right of access requests (SARs)

3.1. Article 15 of the UK GDPR gives individuals the right to obtain a copy of their personal data from us, as well as other supplementary information. It helps individuals to understand how and why we are using their data, and check we are doing it lawfully.

3.2. Some requests may involve personal data about third parties, such as ICO staff, which may need to be considered for disclosure. For example, if someone asks for copies of correspondence in connection with a complaint they submitted, the information may include personal data of ICO employees.

3.3. It is worth noting that information held on corporate systems such as Microsoft Teams and your personal ICO OneDrive accounts may fall in scope of a subject access request if it contains the personal data of the requester, and will need to be considered for disclosure if so.

3.4. In making a decision on the disclosure of ICO employee personal data we will take into account our published guidance: What should we do if the request involves information about other individuals? Where we do not have consent for disclosure, the key question we must consider is whether it is reasonable to comply with the request without that individual's consent.

3.5. Where employees are public-facing (ie they have regular interactions with the public) and their details are already known to the requester, it's usually reasonable to share their information. This could include the name and phone number of the staff member handling a complaint, or others involved in the decision-making who have engaged directly with the requester, such as the officer conducting a case review. This will be done in

line with the ICO's corporate position on how public facing staff sign off their correspondence externally.

3.6. We generally won't share names or contact details of staff who haven't had direct contact with the requester, or who have only had incidental contact with the requester, (for instance taking a call on the helpline), unless they were involved in decisions about the case. We also withhold nicknames, shortened names (diminutives), and details contained in signature blocks; such as working patterns or memberships of internal staff networks, unless the requester already knows them.

3.7. We must also take into account that in recent years identification of individual case officers has led to increasing instances where we have witnessed unacceptable and unreasonable behaviour directed towards our staff. We have a duty to safeguard the health and wellbeing of our staff. The ICO does not expect its staff to tolerate abusive, threatening, demeaning or offensive behaviour either verbally or in writing.

3.8. If there's a risk of such behaviour, we're unlikely to share personal data of ICO staff. This will include consideration of whether the requester is subject to any contact restrictions.

3.9. When we receive a SAR from an existing or former member of staff it is likely to involve a higher degree of sensitivity. As such, these requests are handled outside of ICE in the Information Access restricted access area, so that an appropriate level of confidentiality is in place. We must also consider that, in the circumstances, it is more likely to be reasonable to disclose third party staff information where it is already known to the requester.

Back to the top

4. Proactive and other types of disclosure

4.1. **Proactive disclosure**

We make information available proactively either in line with our transparency obligations or as required by law, for example;

- Executive Team members (ET) and Non-Executive Directors and level H staff members' expenses are published every month,
- renumeration information for ET is published in the annual reports,
- information required to ensure our publication scheme compliance under FOIA, and other relevant legislation such as the The Trade Union (Facility Time Publication Requirements) Regulations 2017 and Public Sector Equality Duty (PSED). Further information can be found on the Trade union facility time and Equality and diversity sections of our website.
- organograms showcasing our management board and decision making structure
- register of interests for the management board,
- blogs and recordings of speaking engagements for staff with public facing roles,
- disclosure of internal speaking engagements and blogs on IRIS and similar platforms,
- main boards and committees' minutes of meetings,
- recordings of workshops and conference presentations, and
- signatories to formal notices (eg decision notices) are usually routinely published where it is appropriate to do so.
- Where an individual has asked for the name and telephone number of your line manager in the course of your dealings with them, this information can usually be provided as normal course of business unless there is good reason not to (see part 3 of the policy).

This is not an exhaustive list.

4.2. **Data sharing**

Disclosure of employee personal data, both internally and externally, in other contexts, (for instance, the information we share about you with HMRC for the purpose of collecting tax and

national insurance contributions etc) is covered in more detail in our Staff Privacy Notice and our personal data sharing policy.

4.3. When Information Access receive a data sharing request from another organisation, they will ensure a lawful basis to share information is identified and will carefully consider the extent to which it is 'necessary' to disclose staff information as part of any disclosure made.

4.4. As explained in section 2, your information may be shared with the Information Access Team, in order to be considered for disclosure in response to information requests. If this information cannot be anonymised, concerns specific individuals and is sensitive in nature it will usually be processed in the Information Access Team 'restricted access' area.

5. Objections to disclosure

5.1. If you have any concerns, or objections, to disclosure of your personal data in any of the above contexts, and in particular if any harm or distress is likely to be caused by disclosure, you should notify HR via Workday, and an Information Access Team manager who can be contacted individually, or through [redacted]

5.2. This can be done proactively at any time and does not have to be in done in connection with a specific information request received by the ICO.

5.3. HR will collate this information and ensure the Information Access Team are notified, if you have not already contacted a manager in Information Access.

5.4. You also have the formal right to object to processing under article 21 of the UK GDPR. These requests will be considered by the Information Access Team. An objection to processing can be made at any time.

5.5. However, if we receive an objection after receipt of an FOI request, the objection will not apply under article 21. This is because on receipt of a request we are under a legal obligation to

respond. Nonetheless, your views on disclosure will be taken into account.

5.6. If we have received a valid objection to processing, then the decision on disclosure is subject to the public interest test. Please see our guidance on section 40 and the right to object for more information.

5.7. Should you wish to exercise your right to object, or any of your other individual rights under the UK GDPR, requests can be submitted to the Information Access Team for consideration by emailing accessicoinformation@ico.org.uk or dpo@ico.org.uk.

5.8. Any such requests are not processed on ICE360. They will be processed in the Information Access Team 'restricted case' area of EDRM in line with their 'restricted cases' procedure.

Back to the top

Feedback on this document

If you have any feedback on this document, please use this form to provide it.

Back to the top

Version history

Version	Changes Made	Date	Made by
0.1	New document created	13/11/2025	[redacted]
0.2	Various changes made based on consultation feedback	30/01/2026	[redacted]
0.3	Tracked changes made in v0.2 accepted	30/01/2026	[redacted]

1.0	Final version for publication	16/02/2026	[redacted]

Back to the top