

8 October 2024

Case reference: IC-331896-T1F3

We are now in a position to respond to your information request of 17 September.

Request

You asked the following:

"February last year you informed... you were "currently working on putting together a formalised process specifically for reprimands, which will be added to our Investigations Manual once finalised" (response to IC-209443-D4K2).

Do you now hold this information (ie has it been finalised)? If so, please may I have a copy?."

We have handled your request for recorded information under the Freedom of Information Act 2000 (FOIA).

Our response

Please find enclosed information within scope of your request. This is the 'Reprimand process checklist' and linked 'Reprimand redaction process' used by the investigations team. These are internal documents for staff on preparing and issuing the reprimand notice of intent (NOI), final notices and redactions prior to publication. The decision on whether a reprimand is appropriate is taken on a case by case basis.

Some of the information has been redacted and further detail on the relevant exemptions are provided below.

Section 40(2) FOIA

Section 40(2) of the FOIA allows a public authority to withhold information from a response to a request when the information requested is personal data relating to someone other than the requestor, and its disclosure would contravene one of the data protection principles. You can read our policy on the disclosure of ICO employee information [here](#).

Section 31(1)(a) FOIA

A small amount of information has been redacted under 31(1)(a) of the FOIA. This is information that relates to our internal information management systems which, if disclosed, would be likely to compromise the security of these and leave us vulnerable to criminal activity by malicious actors.

Section 31(1)(a) of FOIA states that:

'Information... is exempt information if its disclosure under this Act would, or would be likely to, prejudice- (a) the prevention or detection of crime...'

As stated in our guidance, this covers, 'all aspects of the prevention and detection of crime' and can be used to 'withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures...'

As a data controller, we have a duty to safeguard the information that we hold. The 'security principle' of the UK GDPR, states that a data controller must process personal data securely by means of appropriate technical and organisational measures. These measures must ensure the confidentiality, integrity and availability of systems and services and the information processed within them.

We consider that disclosure of this information would be likely to prejudice our effectiveness as a data controller and compromise our ability to protect the information we hold.

The exemption at section 31 is not absolute, and we need to consider the public interest test by weighing up the factors for and against disclosure of the information, as well as any prejudice or harm which may be caused by disclosure. We have considered the public interest test for and against disclosure.

In this instance, the public interest factors in favour of disclosure are:

- Increased transparency in the way in which the ICO holds and processes information.

The public interest factors in favour of maintaining the exemption are:

- There is a strong public interest in the ICO maintaining the security and integrity of the information it holds.

- The risk that, if disclosed, such information could be used by malicious actors seeking criminal access to our information and systems.

Having considered all of these factors, we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

Section 31(1)(g) FOIA

We have redacted an internal email address pursuant to section 31 of the FOIA. This exemption refers to circumstances where the disclosure of information, 'would, or would be likely to, prejudice...the exercise by any public authority of its functions for any of the purposes specified in subsection (2).'

In this case, the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c) which state:

- 'a. the purpose of ascertaining whether any person has failed to comply with the law, and
- c. the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise.'

We are satisfied that any misuse of internal non-public facing email addresses that exist to support ICO staff would likely prejudice our ability to perform our regulatory functions. Public disclosure would leave the email address vulnerable to phishing or other cyber-attacks, spam, or an increased volume of irrelevant correspondence which would divert resources at the expense of assisting staff in matters of information security.

There are other channels that are more appropriate for the public to contact us through. These contact details are publicly available via our website.

The exemption at section 31(1)(g) is not absolute. When considering whether to apply it in response to a request for information, there is a 'public interest test'. That is, we must consider whether the public interest favours withholding or disclosing the information.

In this instance, the public interest factors in favour of disclosing the information are as follows:

- Increased transparency in the way in which the ICO conducts its operations.

The public interest factors in maintaining the exemption are as follows:

- Internal email addresses being utilised for purposes contrary to their intended purpose will reduce the effectiveness and efficiency of our regulatory functions.
- Disclosure of the information is not a critical part of the procedure or of primary relevance to the request.
- The public interest relating to transparency is met by the provision of several other and more appropriate means of contacting the ICO.

Having considered all of these factors, we have taken the decision that the public interest in withholding the information outweighs the public interest in disclosing it.

This concludes our response to your request. We hope you found this information helpful.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days. You can read a copy of our full [review procedure](#) on our website.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority. You can [raise a complaint](#) through our website.

Your information

Our [privacy notice](#) explains what we do with the personal data you provide to us, and sets out [your rights](#). Our [Retention and disposal policy](#) details how long we keep information.

Yours sincerely



Information Access Team
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water
Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews

For information about what we do with personal data see our [privacy notice](#)