The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

12 March 2024

**IC-290720-D5Y9**

## Request

You asked us for information relating to a data breach reported to the ICO by Esher Sixth Form College.

We received your request on 23 February 2024.

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

## Our response

We can confirm that we hold information in scope of your request. The ICO received a data breach report from Esher Sixth Form College on 10 February 2024. I can advise that we did not take any formal regulatory action in relation to this data breach. However, we are unable to disclose the requested information to you as the information is exempt from disclosure.

The information that the data controller has shared with us is exempt by virtue of section 44 (prohibitions on disclosure) of FOIA and the information we have sent in return is exempt by virtue of section 31 (prejudice to law enforcement) of FOIA.

Further details about these exemptions can be found below.

## Section 44 FOIA

Section 44 is an absolute exemption and not subject to a public interest test.

Section 44(1)(a) of the FOIA states:

*"(1) Information is exempt information if its disclosure (otherwise than under this Act) by the public authority holding it is prohibited by or under any enactment."*

In this case, the Data Protection Act 2018, part 5, section 132 prohibits the disclosure of confidential information that:

*"(a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,*
*(b) relates to an identified or identifiable individual or business, and*
*(c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority."*

Section 132(3) imposes a criminal liability on the Commissioner and their staff not to disclose information relating to an identifiable individual or business for the purposes of carrying out our regulatory functions, unless we have the lawful authority to do so, or it has been made public from another source.

We do not consider that we have lawful authority to disclose the information which has been provided to us in confidence in our capacity as a regulatory authority.

**Section 31(g) FOIA**

This exemption applies when disclosure would or would be likely to prejudice our ability to carry out our regulatory function.

The exemption at section 31(1)(g) of the FOIA 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)."*

The purposes referred to in sections 31(2)(a) and (c) are –

*"(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…"*

This exemption is not absolute, and we must consider the prejudice or harm which may be cause by disclosure. We must also carry out a public interest test to weigh up the factors in favour of disclosure and those against.

I consider that disclosure is likely to prejudice the exercise of the ICO's regulatory functions.

Disclosing information in relation to data breach reports or security incidents is likely to dissuade organisations from reporting these incidents in the future. This is because such breach reports and associated outcomes contain sensitive information which is provided to the ICO in confidence. The ICO relies on the co-operation of data controllers, and we feel this is best achieved by an open, voluntary, and uninhibited exchange of information with these organisations. If a data controller, or any other person, believes that information that they provide to us will be shared with the public, it could make organisations reluctant to engage with the ICO in the future.

This could lead to the information gathering process becoming more difficult for the ICO, which makes it harder for us to function as a regulator. We need to provide assurance that details we receive as well as information that we generate in the process of handling a data breach incident are treated securely and used for regulatory purposes. If there is less trust in the ICO's practices, this will put the ICO in a weaker position to monitor, respond and make decisions.

With this in mind, I have now considered the public interest test for and against disclosure.

The public interest factors in favour of disclosing the information are –

- increased transparency in the way in which we carry out our investigations

- the understandable interest of the public, and the data subjects affected by this incident in the details of the data breach.

The public interest factors in maintaining the exemption are –

- the public interest in maintaining an organisations' trust and confidence that breach-related information will be afforded an appropriate level of confidentiality so that they, and other data controllers, feel comfortable sharing information with the ICO

- the public interest in organisations being open and honest in their correspondence with the ICO without fear that it will be made public

- the public interest in maintaining the ICO's ability to carry out enquiries and investigations, on the basis of full, precise details received or obtained from organisations

- the public interest in maintaining the ICO's ability to conduct the investigation into complaints as it thinks fit.

Having considered the arguments both for and against disclosure we do not find that there is sufficient weight in the arguments that favour disclosure. We consider that we need a 'safe space' in which to fulfil our regulatory function and to determine any regulatory action we may choose to take, without undue external influence.

Disclosure of the requested information would be likely to be prejudicial to our regulatory function as it would impact upon our ability to effectively carry out investigations of this nature both now and in the future.

This concludes our response to your request.

**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