



Scottish Information  
Commissioner  
[www.foi.scot](http://www.foi.scot)

# Decision Notice 296/2025

---

## Data incident

Authority: General Teaching Council for Scotland  
Case Ref: 202500109

### Summary

The Applicant asked the Authority for information relating to a data incident which occurred on 3 September 2024. The Authority disclosed some information but withheld other information under exemptions relating to the effective conduct of public affairs. The Commissioner investigated and found that the Authority was only entitled to withhold some information from the Applicant. The Commissioner required the Authority to disclose the wrongly withheld information to the Applicant.

### Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1), (2) and (6) (General entitlement); 30(b)(ii) and (c) (prejudice to effective conduct of public affairs)

### Background

1. On 27 October 2024, the Applicant made a request for information to the Authority. He referred to a data incident which occurred on 3 September 2024 and asked for:

“... a copy of all information held by the [the Authority] in relation to this data incident including what happened, what action was taken to rectify matters and what action has been taken to ensure this type of incident does not happen again on the grounds that it's in the public interest that that the Register is always accurate and when it's not the public has a right to know why not and what is being done about it.”

2. The Authority responded on 21 November 2024. It disclosed some information to the Applicant and withheld other information under the exemptions in sections 30(b)(ii), 30(c) and 38(1)(b) of FOISA.
3. On the same date, the Applicant wrote to the Authority requesting a review of its decision. He stated that he was dissatisfied with the decision because he disagreed with the application of the exemptions in sections 30(b)(ii) and 30(c) of FOISA and because he believed that the Authority held more information relevant to his request.
4. The Authority notified the Applicant of the outcome of its review on 20 December 2024. It disclosed some further information to the Applicant (subject to the redaction of third party personal data under the exemption in section 38(1)(b) of FOISA). However, it did not appear to reconsider the application of the exemptions in sections 30(b)(ii) and 30(c) of FOISA.
5. On 15 January 2025, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA. He stated that he was dissatisfied with the outcome of the Authority's review because he did not agree that the exemptions in sections 30(b)(ii) and 30(c) of FOISA applied.

## Investigation

6. The Commissioner determined that the application complied with section 47(2) of FOISA and that he had the power to carry out an investigation.
7. On 7 February 2025, the Authority was notified in writing that the Applicant had made a valid application. The Authority was asked to send the Commissioner the information withheld from the Applicant. The Authority provided the information, and the case was allocated to an investigating officer.
8. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. The Authority was invited to comment on this application and to answer specific questions, related to its application of the exemptions in sections 30(b)(ii) and 30(c) of FOISA.
9. The Commissioner is considering the withheld information in a single document ("Document 1"). During the investigation, the Authority confirmed that it had not applied the exemptions in sections 30(b)(ii) and 30(c) of FOISA to the same information in Document 1. In other words, the Authority either solely withheld information in Document 1 under the exemption in section 30(b)(ii) of FOISA or solely under the exemption in section 30(c) of FOISA. (The Applicant did not challenge the application of the exemption in section 38(1)(b), so the Commissioner will not consider this in his decision notice.)
10. The Commissioner is aware that explaining his reasoning with specific reference to the withheld information would inevitably disclose details of the withheld information. As the Court of Session recognised in [Scottish Ministers v Scottish Information Commissioner \[2007\] CSIH 8](#)<sup>1</sup> (at [18]):  
  
"It is important, in our view ... to bear in mind that the [Commissioner], in giving reasons for his decision, is necessarily restrained by the need to avoid, deliberately or accidentally, disclosing information which ought not to be disclosed."

---

<sup>1</sup> [https://www.bailii.org/scot/cases/ScotCS/2007109/CSIH\\_8.html](https://www.bailii.org/scot/cases/ScotCS/2007109/CSIH_8.html)

11. As far as he can without revealing the content of information that is withheld, the Commissioner will explain his reasons below.

## **Commissioner's analysis and findings**

12. The Commissioner has considered all of the submissions made to him by the Applicant and the Authority.

### ***Section 30(b)(ii) of FOISA – substantial inhibition to free and frank exchange of views***

13. Section 30(b)(ii) of FOISA provides that information is exempt information if its disclosure would, or would be likely to, inhibit substantially the free and frank exchange of views for the purposes of deliberation. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.
14. In applying the exemption in section 30(b)(ii), the chief consideration is not whether the information constitutes opinion or views, but whether the disclosure of that information would, or would be likely to, inhibit substantially the free and frank exchange of views. The inhibition must be substantial and therefore of real and demonstrable significance.
15. Each request must be considered on a case-by-case basis, taking into account the effect (or likely effect) of disclosure of that particular information on the future exchange of views. The content of the withheld information will require to be considered, taking into account factors such as its nature, subject matter, manner of expression, and also whether the timing of disclosure would have any bearing.
16. As with other exemptions involving a similar test, the Commissioner expects authorities to demonstrate a real risk or likelihood that actual inhibition will occur at some time in the near future, not simply a remote or hypothetical possibility.

### ***The Authority's submissions on section 30(b)(ii)***

17. By way of background, the Authority said that the incident and the circumstances that surrounded it had been explained to the Applicant on multiple occasions – including through a full and comprehensive response provided by its Chief Executive and Registrar in response to a complaint he had made.
18. The Authority considered that the management of a data incident was an inherently sensitive matter which could involve significant risks to data subjects “financial, economic, social and personal lives”. The ability to navigate these risks effectively was contingent on maintaining the privacy needed for open discussion within the relevant team.
19. The Authority said that these are “frequently evolving circumstances” requiring decisive action within the 72 hours allotted by the UK Information Commissioner’s Office for the reporting of incidents to their office. Disclosure of records covering this procedure, and principally the detailed discussions and analysis carried out by the team, beyond what had already been disclosed in this instance, would, according to the Authority, go beyond a reasonable level of disclosure to compromise an inherently sensitive and risk intensive process.
20. The Authority also considered that disclosure of the withheld information in question would limit its ability to engage colleagues in a “discursive problem-solving process”. It said that data incidents are inherently sensitive topics, both for the data subjects involved but also for

the organisation whose processes, systems or resources have resulted in the incident, with a great deal of risk attached to them. It considered that to be more open than it already had on this matter, would prejudice its ability to engage in these kinds of discussions in the future.

21. The Authority considered that, for the proper functioning of its digital incident reporting system, that sensitive information regarding third parties and their special category data should be withheld to ensure the system operated effectively.
22. The Authority submitted that it was it relevant to withhold the withheld information in question, to allow colleagues to come forward with sometimes difficult admissions or explanations on how a particular data incident occurred. If colleagues could not trust that information was given in confidence, then the Authority submitted that it would have effectively prejudiced its ability to handle data incidents in the future.
23. The Authority also stated that it was necessary for any future remediation that the reporting and administration of data incidents be processed discreetly, where necessary. It submitted that open discussion and assessment of issues that had arisen were essential elements of its data incident considerations and disclosure of this information would substantially inhibit any future free and frank sharing of views for the purpose of deliberation in this way and would significantly undermine its data incident management.
24. In terms of who would be likely to be substantially inhibited from providing or exchanging views if the withheld information were disclosed, the Authority explained that it relied on various members of its organisation to input into data incidents. As a result, if colleagues were aware of the disclosure of this type of information, they would be inhibited from contributing in the future if they thought that their contributions would be disclosed under FOISA. It argued that this would be organisation wide and would have a detrimental impact on its management of data incidents. It said that disclosure of the deliberations contained in the withheld information would have a “chilling effect” on staff, who need to be able to have free and frank discussions about what happened in a private space in order to ensure incidents are fully investigated.
25. The Authority submitted that colleagues need to feel able to respond to data incidents at an early stage, to enable a thorough assessment of the matter arising and without fear of getting it wrong or of their future public disclosure. It said that such information is often sensitive and protecting the sharing of views of those involved in the incident, to ensure that it manages the incident effectively, is essential to its data incident reporting process.
26. The Authority considered that the risk of inhibition is that, in the absence of clear indicators of how an incident occurred, contributors might be hesitant to volunteer opinions and views and so deprive the organisation of unrestrained considerations on developing circumstances which might carry risk for the individual volunteering the information. To ensure that staff are not inhibited from contributing to its incident reporting, the Authority considered it appropriate to withhold the information in question under the exemption in section 30(b)(ii) of FOISA to maintain the confidentiality of its digital incident reporting procedures.

*The Applicant’s submissions on section 30(b)(ii)*

27. The Applicant disagreed that the exemption in section 30(b)(ii) of FOISA applied and, if it did, he considered that the public interest favoured disclosure of the withheld information.

*The Commissioner's view on section 30(b)(ii)*

28. The Commissioner has carefully considered the withheld information, together with the submissions from the Applicant and the Authority.
29. The Commissioner acknowledges that withheld information in question contains views. However, as noted above, the primary consideration is not whether the information contains views, but whether its disclosure would have, or would be likely to have, the substantially inhibiting effect specified in section 30(b)(ii) of FOISA.
30. Having carefully considered the withheld information, the Commissioner is not satisfied that the withheld information would give, or be likely to give, rise to the prejudice claimed by the Authority (or required to engage the exemption in section 30(b)(ii) of FOISA). Most of the withheld information contains views expressed in relatively measured, non-contentious or benign terms.
31. The Commissioner accepts that the Authority must (in appropriate circumstances) have a confidential space in which to respond to data incidents and for staff to respond to such incidents (and to develop and test its information security and data protection practices).
32. However, the Commissioner is not persuaded that disclosure of the withheld information would, or would be likely to, given its nature and the legal duty to respond to data incidents, act to inhibit employees of the Authority from recording similar information in future or contributing to the response to a future data incident to the extent that there would be a meaningful "chilling effect" on the Authority's ability to effectively respond to and manage such incidents. In fact, he considers it unlikely that disclosure of the withheld information in question would, or would be likely to, substantially inhibit future free and frank sharing of views for the purpose of deliberation or that it would significantly undermine its data incident management.
33. While the Commissioner accepts that information relating to a data incident (and a public authority's response to it) can, depending on the circumstances, be sensitive, he is not persuaded that the withheld information in question is. If the withheld information were disclosed, he does not consider that it would reveal anything of particular sensitivity – either about the incident itself or the Authority's response to it.
34. However, the Commissioner would like to stress that it is important for public authorities to treat each request for information on a case-by-case basis. That information should be disclosed in one case should not be taken to imply that information of a particular type will be routinely disclosed in future. The circumstances of each case, including the content of the specific information under consideration, must be taken into consideration and (where required) the public interest in each case assessed on its own merits.
35. In all of the circumstances, based on the submissions provided and having carefully considered the withheld information, the Commissioner does not accept that disclosure of this information would, or would be likely to, inhibit substantially the free and frank exchange of views for the purposes of deliberation.
36. For these reasons, the Commissioner concludes that the Authority was not entitled to withhold the information in this case under the exemption in section 30(b)(ii) of FOISA. Given this conclusion, he is not required to go on to consider the public interest test in section 2(1)(b) of FOISA. He requires the Authority to disclose this information to the Applicant.

### ***Section 30(c) – prejudice to the effective conduct of public affairs***

37. Section 30(c) of FOISA exempts information if its disclosure “would otherwise prejudice substantially, or would be likely to prejudice substantially, the effective conduct of public affairs”.
38. The use of the word “otherwise” distinguishes the harm required from that envisaged by the exemptions in sections 30(a) and (b). This is a broad exemption, and the Commissioner expects any public authority citing it to show what specific harm would (or would be likely to) be caused to the conduct of public affairs by the disclosure of the information, and how that harm would be expected to follow from disclosure.
39. There is no definition of “substantial prejudice” in FOISA, but the Commissioner considers the harm in question would require to be of real and demonstrable significance. The authority must also be able to satisfy the Commissioner that the harm would, or would be likely to, occur: therefore, the authority needs to establish a real risk or likelihood of actual harm occurring as a consequence of disclosure at some time in the near (certainly the foreseeable) future, not simply that the harm is a remote possibility.
40. This exemption is subject to the public interest test in section 2(1)(b) of FOISA.

#### *The Authority's submissions on section 30(c)*

41. The Authority explained that the records detailing the assessment of the incident, remediation and other information associated with the incident had been provided to the Applicant “with relatively minimal redactions”.
42. The Authority said that it had applied the exemption in section 30(c) of FOISA where it considered disclosure of this information would limit its ability to effectively manage data incidents. More specifically, it considered that disclosure of this information could expose the Authority to digital risks.
43. While the Authority considered it had provided as much information as it considered “appropriate and necessary” in response to the request, it considered that information which discussed measures put in place to protect the integrity of the data to be sufficiently sensitive that its disclosure would expose the Authority to risk that would prejudice its effective conduct.
44. The Authority submitted that information of this nature would be useful to a “motivated intruder looking for vulnerabilities which could be exploited by a malicious actor” and that an individual with relevant IT skills “could potentially utilise this information to jeopardise our information security”.
45. Taking all of this into consideration, the Authority considered that disclosure of this information could seriously undermine its data protection and data integrity measures, as well as its “internal improvement and development work” in relation to the management of the personal and other data it held.
46. The Authority considered that the impact of disclosing the information would be “significant” and that it should have a confidential space in which its information security and data protection practices can be tested and improved without risk of these being disclosed to the public.
47. In terms of future digital risk reporting, the Authority viewed that disclosure was likely to substantially prejudice and harm the effectiveness of this, by prejudicing both the submission

and consideration of inherently sensitive information related to the personal data of third parties.

48. The Authority explained that it considered that there were inherent risks in it disclosing platforms and systems used for records management and storage, which would highlight for “malevolent actors” where they would wish to target a large volume of sensitive personal data should they wish to do so.
49. From a digital security perspective, the Authority also considered it a risk to disclose those third parties with whom it shared sensitive personal data and large volumes of data. The Authority considered this could highlight where it could be targeted in terms of cyber-attacks within the context of data sharing.
50. The Authority argued that there was an inherent risk in disclosure of information that detailed the incident in question and other data incidents when discussing potential vulnerabilities in its systems that it was seeking to address effectively.
51. The Authority also submitted that disclosure of the withheld information would have a similar “chilling effect” to that described to the information withheld under the exemption in section 30(b)(ii) of FOISA. Rather than affecting the free and frank nature of discussions, staff would be likely to feel significantly inhibited from recording facts fully relating to a data incident, if there was a likelihood that they would be disclosed into the public domain in future.

*The Applicant’s submissions on section 30(c)*

52. The Applicant disagreed that the exemption in section 30(c) of FOISA applied and, if it did, he considered that the public interest favoured disclosure of the withheld information.

*The Commissioner’s view*

53. The Commissioner has carefully considered the withheld information, together with the submissions from the Applicant and the Authority.
54. Having carefully considered the withheld information, the Commissioner is not satisfied that most of that information would give, or be likely to give, rise to the prejudice claimed by the Authority (or required to engage the exemption in section 30(b)(ii) of FOISA).
55. Most of the withheld information is not particularly sensitive and simply describes in uncontroversial terms the Authority’s response to the data incident in question or contains suggestions that are sensible or predictable. In some instances, the information that has been withheld has effectively been disclosed elsewhere in the same document by the Authority.
56. While the Commissioner accepts that the Authority must (in appropriate circumstances) have a confidential space in which to test its information security and data protection practices can be tested and improved, he is not persuaded that disclosure of the majority of the withheld information would, or would be likely to, given its nature and what has been disclosed elsewhere, either act to inhibit employees of the Authority from recording similar information in future or result in a motivated and malicious actor jeopardising the Authority’s information security.
57. While the Commissioner has fully considered the Authority’s submissions on the prejudice that is considered would, or would be likely to, arise as a result of disclosure of the withheld information, the Commissioner is, in the main, not persuaded by these submissions. Regarding how disclosure of this information would permit, or result in, a motivated and

malicious actor jeopardising the Authority's information security, the Commissioner is not satisfied that the Authority has adequately explained how the prejudice required for the exemption in section 30(c) of FOISA would, or would be likely to, arise.

58. However, the Commissioner accepts that disclosure of a small amount of information that is more specific in nature could expose the Authority to the digital risks it described above – specifically, that from a digital security perspective it would highlight where the Authority could be targeted in terms of cyber-attacks within the context of data sharing. In the circumstances, he accepts that this information was properly exempted under section 30(c) of FOISA.
59. The Commissioner is not required to consider the public interest test in section 2(1)(b) of FOISA in relation to the information to which he has found the exemption in section 30(c) does not apply. He requires the Authority to disclose this information to the Applicant.
60. However, the Commissioner will now go on to consider the application of the public interest test to the information to which he has found the exemption in section 30(c) does apply.

### ***The public interest test – section 30(c)***

61. The “public interest” is not defined in FOISA but has been described as “something which is of serious concern and benefit to the public”, not merely something of individual interest. The public interest does not mean “of interest to the public” but “in the interest of the public”, i.e. disclosure must serve the interests of the public.

### ***The Authority's submissions on the public interest***

62. The Authority noted that in his [Decision 295/2024](#)<sup>2</sup>, the Commissioner found (at paragraph 50) that  
“... there is always a general public interest in openness and accountability. Openness and accountability allow effective scrutiny and reassure the public, where appropriate.”
63. The Authority agreed with the Applicant's position that it was in the public interest to ensure the Register is always accurate and said that it welcomed the right of the public to view the publicly available information on the Register for their own purposes. It noted that it is legally required to ensure that the Register is available for public inspection – a requirement it said that it embraced, and that it does all it can to ensure the Register is easily accessible to the public.
64. The Authority explained that, in relation to the incident referred to in the Applicant's request, a data error had occurred, been identified and managed. It said that at no point did any of the registrants involved lose their registration with the Authority, that they always remained registered with the Authority and that it held (and continued to hold) their records as registrants.
65. The Authority said that the error in question occurred as a result of human error – a simple spelling error which was resolved fairly quickly. It said that it saw no significant public interest in this matter beyond the Applicant's personal interest. Specifically, it considered that the Applicant was insistent on pursuing this request because of his distrust of the

---

<sup>2</sup> <https://www.foi.scot/decision-2952024>

Authority and his belief that the spelling error was evidence of a conspiracy instead of an administrative error.

66. The Authority noted that no other requester had asked for this information. As such, it believed that it was contrary to the public interest to make certain details of its procedure in the case of data incidents public knowledge when disclosure of that information was not of significant interest to the public generally.
67. The Authority deemed that to withhold the information in question and ensure the continued free and frank exchange of views for the purpose of deliberation, was in the public interest. This ensured that its data incident management processes were robust and thorough. In the Authority's view, that outweighed the public interest in the release of this information.
68. The Authority also referred to paragraph 31 of [Decision 052/2024](#)<sup>3</sup> of the Commissioner, where he acknowledged the risk of substantial prejudice to the effective conduct of public affairs when disclosure affects "the open engagement of all parties in the investigation process and thereby the value of these investigations."
69. The Authority explained that its digital incident reporting, similarly, investigated the circumstances under which an incident occurred and how it might be prevented in the future. It argued that disclosure of the withheld information in question would be more likely to compromise the investigative process than provide any further transparency than it had already given.
70. Ultimately, the Authority considered that disclosure of the withheld information in question would more likely harm the public interest than serve it. However, as a responsible regulator, it recognised transparency as an important part of its work and had provided records to the requester. For the "nominal redactions" it had applied, the Authority did not consider that the public interest in disclosure outweighed that in upholding the exemption.

#### *The Applicant's submissions on the public interest*

71. The Applicant explained that his request related to a registered teacher whose name could not be found on the teaching register, just before serious allegations about their conduct were to be made to the Authority.
72. The Applicant said that did not accept the explanation provided by the Authority relating to how the error occurred relating to the teacher's name not being found on the register. He explained that he (and others) believed that the Authority was "operating in non-transparent ways" and argued that the public needed more, not less, transparency from the Authority (who he considered was not adequately and effectively investigating teachers).

#### *The Commissioner's view on the public interest*

73. The Commissioner has carefully considered the nature of the remaining withheld information and the submissions from the Applicant and the Authority.
74. The Commissioner recognises the general public interest in transparency and accountability, particularly where disclosure of information might contribute to understanding the integrity of the teaching register or how the Authority responds to data incidents.

---

<sup>3</sup> <https://www.foi.scot/sites/default/files/2024-05/Decision052-2024.pdf>

75. However, the remaining withheld information is very specific in nature. At most, the Commissioner considers there to be a very limited public interest in disclosure of this information as it would not contribute in any meaningful way to understanding the integrity of the teaching register or how the Authority responds to data incidents.
76. The Commissioner has already accepted, on balance, that disclosure of the remaining withheld information was properly withheld under the exemption in section 30(c) of FOISA.
77. Given the specific nature of the remaining withheld information and the very limited public interest in its disclosure, the Commissioner is satisfied, in all of the circumstances, that the public interest in disclosure is outweighed by that in maintaining the exemption and allowing the remaining withheld information to be withheld under the exemption in section 30(c) of FOISA.
78. The Commissioner therefore finds that the Authority was entitled to withhold the remaining withheld information under this exemption.

### ***Other matters***

79. As stated above, the Authority confirmed during the investigation that it had not applied the exemptions in sections 30(b)(ii) and 30(c) of FOISA to the same information in Document 1. At the same time, the Authority requested the opportunity to respond to “invoke the alternative appropriate section 30 exemption” if the Commissioner did not agree with its application of different section 30 exemptions in FOISA to the withheld information.
80. While section 49(3) of FOISA requires the Commissioner to notify an authority that an application has been received, and to invite comments from an authority, it does not require him to revert to an authority to provide it an additional opportunity to apply an alternative exemption should he find that the exemption initially cited did not apply.
81. When inviting comments from authorities, the Commissioner states the following:

“This is your opportunity to provide any comments in support of your position and the Commissioner will issue a decision based on these. The decision may require the disclosure of any withheld information. Please prepare your comments with this in mind. Only in exceptional circumstances will you be given the opportunity to provide any further comments.”
82. The Commissioner would remind all authorities that when he invites their comments on an application (as he is required to do by section 49(3) of FOISA) to ensure that they include all of the arguments they wish to make to support their case, as they may not be given any further opportunities to comment.

## **Decision**

The Commissioner finds that the Authority partially complied with Part 1 of the Freedom of Information (Scotland) Act 2002 (FOISA) in responding to the information request made by the Applicant.

The Commissioner finds that by relying on the exemption in section 30(c) of FOISA to withhold some information, the Authority complied with Part 1.

However, by wrongly withholding information under the exemption in section 30(b)(ii) and other information under the exemption in section 30(c) of FOISA, the Authority failed to comply with Part 1 (specifically section 1(1)).

The Commissioner therefore requires the Authority to provide the Applicant with the information wrongly withheld, by **26 January 2026**. He will provide a marked-up copy of the withheld information to the Authority indicating what information should be disclosed.

## **Appeal**

Should either the Applicant or the Authority wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

## **Enforcement**

If the Authority fails to comply with this decision, the Commissioner has the right to certify to the Court of Session that the Authority has failed to comply. The Court has the right to inquire into the matter and may deal with the Authority as if it had committed a contempt of court.

**Euan McCulloch**  
**Head of Enforcement**

**12 December 2025**