

Our Ref: FOI 17130
Your Ref: FOI 17339
Date: 12 November 2024

Internal Review

Re: Request for internal review of response to application for information under the provisions of the Freedom of Information Act 2000, original request first notified to Staffordshire Police on 09/10/2024.

We refer to the above request which was expressed in the following terms:

I am writing to respectfully request the disclosure of information under the Freedom of Information Act 2000. Specifically, I am seeking the disclosure of any data or information held by the force that details the organisations and/or individuals recognised by the Chief Constable to install Type A intruder alarm systems within your jurisdiction.

This request pertains to any records, lists, documents, or databases, whether current or historical, that identify those companies or individuals authorised to install and maintain Type A alarm systems which comply with British Standards (such as BS EN 50131 or BS 4737) and are eligible for police response upon alarm activation.

Public Interest and Pre-emptive Counter to Potential Exemptions:

I recognise that the police may choose to refer the public to the National Security Inspectorate (NSI) or the Security Systems and Alarm Inspection Board (SSAIB) to locate qualified installers. However, my request does not seek an endorsement or recommendation but rather the factual data held by your force regarding those entities or individuals recognised by the Chief Constable under this specific capacity.

I anticipate that arguments may be raised regarding the disclosure of this information under exemptions like Section 31 (Law Enforcement) or Section 43 (Commercial Interests). However, I would like to make the following points in advance:

- 1. Transparency and Accountability:** There is a clear public interest in knowing which installers are recognised by the police, especially given the critical nature of security systems. Disclosure would ensure that your force is acting transparently in its recognition of installers, thus maintaining public confidence in security services.
- 2. Commercial Sensitivity:** The names of organisations or individuals recognised to install Type A alarms do not, in themselves, constitute commercially sensitive information. The public, particularly those seeking to ensure their alarms meet the necessary standards for police response, have a right to access this data to make informed decisions.
- 3. Law Enforcement:** Releasing the list of recognised installers is unlikely to prejudice law enforcement activities. On the contrary, providing clarity on which companies are authorised to install Type A alarms may enhance public safety by ensuring installations meet the required standards, reducing the number of false alarms and unnecessary police responses.

I trust that this request will be handled promptly and in accordance with your obligations under the Freedom of Information Act. Should any part of the requested information be exempt from disclosure, I kindly request that you provide an explanation as to why, and supply all other available data.

If you require any further information to assist with this request, please feel free to contact me. I look forward to your response within the statutory time limit of 20 working days.

Further to the above, we also note the following comments made within your request for Internal Review.

I am writing to request an internal review of Staffordshire Police's handling of my Freedom of Information Act 2000 (FOIA) request dated 9 October 2024, concerning the disclosure of information about organisations and individuals recognised by the Chief Constable to install Type A intruder alarm systems within your jurisdiction.

Background:

On 9 October 2024, I submitted an FOIA request seeking details of entities recognised by the Chief Constable to install Type A intruder alarm systems.

On 30 October 2024, I received a response from your office (reference 17339), which refused to disclose the requested information, citing Section 31(1)(a)(b) of the FOIA—Law Enforcement.

Grounds for Internal Review:

I respectfully challenge the decision to refuse my FOIA request and believe that the refusal is unwarranted under the FOIA. My grounds for requesting an internal review are as follows:

1. Misapplication of Section 31(1)(a)(b) Exemption:

a. Prejudice Not Adequately Demonstrated:

Section 31(1)(a)(b) is a qualified, prejudice-based exemption. To apply this exemption, the public authority must demonstrate that disclosure would, or would be likely to, prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In *John Connor Press Associates Ltd v Information Commissioner* (EA/2005/0005), the Information Tribunal stated that "the public authority must be able to demonstrate that the risk of prejudice is real, actual, or of substance; not simply a remote possibility."

Your response asserts that disclosing the names of specific companies accredited to install Type A alarms would expose vulnerabilities. However, this assertion is speculative and lacks evidential support. The information requested does not reveal sensitive operational details, specific security measures, or the locations of protected sites that could be exploited by criminals.

b. Lack of Causal Link:

The Information Tribunal in *Hogan and Oxford City Council v Information Commissioner* (EA/2005/0026 and EA/2005/0030) emphasised that there must be a causal link between the disclosure and the potential prejudice, and that the prejudice must be more than trivial.

Providing a list of accredited installers does not directly lead to an increased risk of crime. It does not identify which properties are protected by which companies, nor does it disclose any response protocols or vulnerabilities.

2. Public Interest in Disclosure:

a. Promoting Public Safety:

Disclosure of the list enables the public to make informed decisions when selecting alarm installers, ensuring that systems meet required standards. This enhances public safety by reducing the risk of faulty installations and false alarms, which can strain police resources.

b. Accountability and Transparency:

Transparency in the recognition of accredited installers fosters trust between the public and the police. It ensures that the process is open and that only qualified and reputable companies are recognised, thereby promoting industry standards.

3. Inadequate Public Interest Test:

Your response acknowledges the public interest in transparency but does not sufficiently weigh this against the speculative harm proposed. The Information Commissioner's Office (ICO) Decision Notice FS50657694 emphasises that the public interest test must consider both the likelihood and severity of the prejudice, as well as the benefits of disclosure.

The refusal does not provide a detailed analysis of how the public interest in maintaining the exemption outweighs the significant public interest in disclosure.

4. Information Already in the Public Domain:

a. Publicly Available Lists:

The National Security Inspectorate (NSI) and the Security Systems and Alarms Inspection Board (SSAIB) already publish lists of accredited installers. Many of these companies openly advertise their accreditation and services.

b. Precedent of Disclosure:

Other police forces have disclosed similar information without adverse effects, indicating that the risk of prejudice is minimal. This inconsistency undermines the argument that disclosure would cause harm.

5. Failure to Consider Section 16 Duty to Advise and Assist:

Under Section 16 of the FOIA, public authorities have a duty to provide advice and assistance to applicants. If there were concerns about disclosing specific details, the authority could have suggested alternative ways to fulfill the request without causing harm.

6. Encouraging Use of Unaccredited Installers:

By withholding this information, the public may inadvertently engage unaccredited or unqualified installers, potentially compromising security and increasing the risk of crime, contrary to the objectives of Section 31.

7. No Evidence of Real Harm:

The claimed harm is hypothetical. There is no evidence to suggest that disclosing the list of recognised installers has led to an increase in crime or has compromised law enforcement activities in other jurisdictions where such information is available.

Request for Internal Review:

In light of the above, I respectfully request that you:

1. Conduct an Internal Review:

Reassess the decision to refuse my request, considering the arguments presented and relevant case law.

2. Reevaluate the Applicability of Section 31(1)(a)(b):

Determine whether the exemption genuinely applies, given the lack of demonstrated prejudice and the strong public interest in disclosure.

3. Provide a Detailed Explanation:

If you maintain the refusal, please provide a comprehensive explanation, including:

- The specific reasons why the exemption applies.
- How disclosure would lead to the claimed prejudice.
- A thorough public interest test that fully considers the benefits of disclosure.

4. Disclose the Requested Information:

If, upon review, it is determined that the exemption does not apply or that the public interest favors disclosure.

Conclusion:

Transparency in this matter aligns with the principles of the FOIA and serves the public interest by promoting safety, accountability, and informed decision-making. The speculative nature of the harm proposed does not outweigh the significant public benefits of disclosure.

I trust that the internal review will be conducted independently and impartially, in accordance with the FOIA and the Section 45 Code of Practice. I look forward to your response within the statutory time limit of 20 working days.

Thank you for your attention to this matter.

Our Response

Upon review of your request for information under the Freedom of Information provision, referenced above, and all corresponding communication, we are of the opinion that the response issued, alongside all clarification provided, fully answers the terms of your request.

We also confirm that the application of all exemptions outlined within this response are fully justified, and that the explanations and rationale for their application conveyed clearly and unequivocally.

However, please find below our response to the specific points raised.

1. Misapplication of Section 31(1)(a)(b) Exemption:

a. Prejudice Not Adequately Demonstrated:

Section 31(1)(a)(b) is a qualified, prejudice-based exemption. To apply this exemption, the public authority must demonstrate that disclosure would, or would be likely to, prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

In *John Connor Press Associates Ltd v Information Commissioner (EA/2005/0005)*, the Information Tribunal stated that “the public authority must be able to demonstrate that the risk of prejudice is real, actual, or of substance; not simply a remote possibility.”

Your response asserts that disclosing the names of specific companies accredited to install Type A alarms would expose vulnerabilities. However, this assertion is speculative and lacks evidential support. The information requested does not reveal sensitive operational details, specific security measures, or the locations of protected sites that could be exploited by criminals.

b. Lack of Causal Link:

The Information Tribunal in *Hogan and Oxford City Council v Information Commissioner (EA/2005/0026 and EA/2005/0030)* emphasised that there must be a causal link between the disclosure and the potential prejudice, and that the prejudice must be more than trivial.

Providing a list of accredited installers does not directly lead to an increased risk of crime. It does not identify which properties are protected by which companies, nor does it disclose any response protocols or vulnerabilities.

Having reviewed our initial response we feel that the harm identified is sufficient and proportionate to apply exemption under Section 31(1)(a)(b).

Whilst we acknowledge that disclosure of this information alone may not reveal sensitive operational details, specific security measures or the exact locations of protected sites; provision of the names of specific companies accredited to install Type A alarms would expose other companies and the buildings protected, making them more vulnerable to attack by persons seeking to gain unauthorised access.

There is therefore, a clear link allowing offenders to identify properties to target by building a picture of accredited installers from those who don't install such alarm types. This would subsequently allow individuals to develop an understanding of which premises may receive a slower response from police; thus, leading to unknown harm and vulnerabilities to properties and therefore the public.

2. Public Interest in Disclosure:

a. Promoting Public Safety:

Disclosure of the list enables the public to make informed decisions when selecting alarm installers, ensuring that systems meet required standards. This enhances public safety by reducing the risk of faulty installations and false alarms, which can strain police resources.

b. Accountability and Transparency:

Transparency in the recognition of accredited installers fosters trust between the public and the police. It ensures that the process is open and that only qualified and reputable companies are recognised, thereby promoting industry standards.

Whilst acknowledging the above statements, the harm vs accountability and transparency has been considered and, in these circumstances, we consider that the harm outweighs the requirement for transparency.

3. Inadequate Public Interest Test:

Your response acknowledges the public interest in transparency but does not sufficiently weigh this against the speculative harm proposed. The Information Commissioner's Office (ICO) Decision Notice FS50657694 emphasises that the public interest test must consider both the likelihood and severity of the prejudice, as well as the benefits of disclosure.

The refusal does not provide a detailed analysis of how the public interest in maintaining the exemption outweighs the significant public interest in disclosure.

In the consideration for disclosure of the information requested, we have considered the public interest regarding transparency but have still deemed that the harm indicated outweighs this.

4. Information Already in the Public Domain:

a. Publicly Available Lists:

The National Security Inspectorate (NSI) and the Security Systems and Alarms Inspection Board (SSAIB) already publish lists of accredited installers. Many of these companies openly advertise their accreditation and services

Whilst we acknowledge that the sites indicated do publish a list of accredited installers and do highlight which force these are linked to; the accreditation and website does not state what type of alarm they install. It could be determined that these websites support transparency in that they allow the public to determine accredited installers. However, that being said, as of this time a list of installers for Type A alarms is still not in the public domain.

b. Precedent of Disclosure:

Other police forces have disclosed similar information without adverse effects, indicating that the risk of prejudice is minimal. This inconsistency undermines the argument that disclosure would cause harm.

The landscape and nature of crime is dynamic can alter quickly, the Precedent of Disclosure cannot therefore be relied upon in perpetuity. To merely state that information has been disclosed previously or in certain areas should not be interpreted as universal. Where required, a full harm test should be considered against each disclosure in light of the hazards such disclosure would pose against the current landscape of crime and offending.

5. Failure to Consider Section 16 Duty to Advise and Assist:

Under Section 16 of the FOIA, public authorities have a duty to provide advice and assistance to applicants. If there were concerns about disclosing specific details, the authority could have suggested alternative ways to fulfil the request without causing harm.

Whilst we acknowledge that Section 16 outlines our obligation to offer advice and assistance, on this occasion, no further advice could be provided to assist with your request.

6. Encouraging Use of Unaccredited Installers:

By withholding this information, the public may inadvertently engage unaccredited or unqualified installers, potentially compromising security and increasing the risk of crime, contrary to the objectives of Section 31.

We refer back to the information in the public domain, accessible via the websites indicated at point 4 above, which provides details of accredited installers.

7. No Evidence of Real Harm:

The claimed harm is hypothetical. There is no evidence to suggest that disclosing the list of recognised installers has led to an increase in crime or has compromised law enforcement activities in other jurisdictions where such information is available.

We refer back to the Harm and Public Interest test provided within our initial response.

Please be advised that all FOI requests and response letters are published on the Staffordshire Police website although personal details are not included.

If you are not content with the outcome of the review, you may apply directly to the Information Commissioner to investigate. The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ICO Website for complaints link: <https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/foi-and-eir-complaints/>

Central Disclosure Unit Management Team
Central Disclosure Unit
Staffordshire Police