

5 February 2026

FOI Ref 22353

Request - You asked Staffordshire Police (SP) the following:

Under the Freedom of Information Act 2000, please provide the following information for the period 1 January 2023 – 31 December 2024:

1. The number of occasions on which cyber or information security risks appeared on the agenda of your governing body (or equivalent oversight body).
2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight.
3. Whether documented criteria exist for escalating significant cyber incidents to the governing body or senior leadership (yes/no; if yes, please provide or summarise).
4. The number of governing body members (or equivalent) who completed cyber or information security training during this period, and the total number of members in that body.
5. Whether an independent assessment of your cyber security arrangements (e.g. internal audit, external review, or third-party assessment) was reported to the governing body during this period (yes/no; if yes, please state the type of assessment).

Please note: no technical details, vulnerabilities, or sensitive operational information are requested. If this information is readily available, broken down by year, please provide it; otherwise, an aggregate figure for the period is sufficient.

Clarification received on 14/01/2026:

For the purposes of this Freedom of Information request, the term “governing body” refers to the principal strategic oversight body or bodies responsible for organisational governance, assurance, and corporate risk within Staffordshire Police.

This should be interpreted to include, as applicable, any of the following during the period 1 January 2023 – 31 December 2024:

- the Chief Officer Group / Executive Board;
- the Force Management Board or equivalent senior leadership forum;
- any formal committee or board with delegated responsibility for strategic risk, assurance, or information and cyber security oversight;
- where relevant, any joint, statutory, or regional oversight body to which cyber or information security matters are escalated at a strategic level.

If responsibility for cyber or information security oversight changed during the period in scope, please apply this definition to the relevant body or bodies in place at the time.

This clarification is provided to enable the request to proceed without narrowing its scope.

SP received your request on 09/01/2026 and have processed this under the Freedom of Information Act (FOIA).

SP's response to your enquiry is as follows:

SP holds/does not hold the requested information.

Under the Freedom of Information Act 2000, please provide the following information for the period 1 January 2023 – 31 December 2024:

- 1. The number of occasions on which cyber or information security risks appeared on the agenda of your governing body (or equivalent oversight body). - **Unknown.** *
- 2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight. – **Disclosed, Security Working Group, Cyber Working Group and Information Assurance Board.**
- 3. Whether documented criteria exist for escalating significant cyber incidents to the governing body or senior leadership (yes/no; if yes, please provide or summarise). – **Disclosed, yes. The force has a Cyber Security Incident Response Plan. Further details would attract Section 24 and Section 31 exemptions.**
- 4. The number of governing body members (or equivalent) who completed cyber or information security training during this period, and the total number of members in that body. - **Unknown.** *
- 5. Whether an independent assessment of your cyber security arrangements (e.g. internal audit, external review, or third-party assessment) was reported to the governing body during this period (yes/no; if yes, please state the type of assessment). – **Disclosed, yes. The force's performance was assessed against the Police Digital Service's Security Assessment for Policing framework (SyAP).**

Please be advised that all Freedom of Information request responses are published on the SP website although personal details are not included.

Advice and assistance

Section 16 of the Act places an obligation upon the Authority to provide advice and assistance, in order to comply with this obligation please see below.

* The Freedom of Information Team have made numerous exhaustive attempts to obtain the data you have requested from the relevant data holders within the force. However, following all attempts, we have been unable to receive a satisfactory response from the data holder with which to provide a response to your request. If you are dissatisfied with the handling of your information request, you can make an appeal to the Information Commissioner's Office (ICO). The easiest way to lodge your appeal is via their website: www.ico.org.uk/foicomplaints

Freedom of Information within the Information Access Team