



**POLICE & CRIME  
COMMISSIONER**  
for Leicester,  
Leicestershire & Rutland  
Your Communities - Your Commissioner

Our ref: FOI 0002/26 – OPCC1017

Date: 05 February 2025

Name:

Email:

Dear

**Freedom of Information Act 2000**

I write further to your freedom of information request received on 8 January 2026. I note you seek access to the following 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).
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.



Your request for information has now been considered, and the response can be found below:

## **Cyber Security Governance 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).**

The Corporate Governance Board (CGB) is the main PCC accountability board holding the Chief Constable to account and oversight of the discussions can be found within the PCC Updates to the Police and Crime Panel. Further information on this meeting is available via the following link: [Leicester, Leicestershire and Rutland Police and Crime Panel](#)

In addition to this, Data Protection appeared frequently within the independent Joint Audit, Risk and Assurance Panel (JARAP). Further information on this meeting is available via the following link: [Joint Audit, Risk and Assurance Panel Meetings](#)

### **2. The name(s) of any committee(s) or board(s) with formal responsibility for cyber or information security oversight.**

See Above

### **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).**

Yes – [Risk Management Policy and Framework](#) . Mechanisms are in place as part of the PCC Risk Register and Financial Risk Regulations to escalate and monitor significant cyber incidents.

### **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.**

All staff undertake mandatory information security training on appointment and have regular refresher training.

### **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).**

Audit reports are generally discussed in JARAP. Please see the meeting link above.

**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.**



If you are not satisfied with our response to your request, under Section 17 of the FOIA you are entitled to ask for an internal review of our decision. Any internal review needs to be submitted within two months of the date of receipt of this response and state why you are unhappy with the response. You can submit an internal review in the following ways:

- Emailing the OPCC Inbox to [OPCC@leics.police.uk](mailto:OPCC@leics.police.uk). or
- Writing to the OPCC at – The Office of the Police and Crime Commissioner for Leicester, Leicestershire and Rutland, Police Headquarters, St Johns, Enderby, Leicestershire, Leicestershire, LE19 2BX
- By phone – 0116 229 8980 (as a reasonable adjustment under the Equality Act 2010).

If you are not satisfied with the outcome of the internal review under Section 50 of the FOIA you can apply directly to the Information Commissioner (ICO) for a decision. Generally, the ICO cannot make a decision unless you have exhausted the internal review procedure provided by the OPCC. You can contact the ICO in the following ways:

- Online at the ICO – <https://ico.org.uk/global/contact-us/>. or;
- Writing to the ICO at –Information Commissioner's Office Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Yours sincerely,

**Office of the Police and Crime Commissioner**