Report: OPCC Data Protection Report 2025/26

Report to: Chair and Members of the Cleveland Joint Audit Committee

Date: Friday 25th September 2026

Status: For information

Presenting Officer: Rachelle Kipling, Head of Policy, Partnerships and Delivery (& Data Protection Officer)

Annual Data Protection Report 2025/26

1. Purpose

The purpose of this report is to provide members of the Cleveland Joint Audit Committee with an update on the Office of the Police and Crime Commissioner (OPCC), Data Protection obligations during the 2025/26 period.

2. Recommendation

That members note the contents of the report.

3. Background

3.1 Police and Crime Commissioners (PCCs) are subject to the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018, which mandates the secure handling of personal data.

3.2 Under GDPR the PCC is the Data Controller. The Chief Executive and Monitoring Officer has delegated authority to carry out all functions and responsibilities of the Data Controller, although liability remains with the PCC as the 'corporation sole'.

3.3 The OPCC is registered with the Information Commissioner's Office (ICO) and ensures compliance with UK GDPR and Data Protection Act 2018 through the duties and responsibilities of the Data Protection Officer. This includes assisting in monitoring internal compliance, informing and advising on data protection obligations, providing advice regarding Data Protection Impact Assessments

(DPIAs) and acting as a contact point for data subjects and the Information Commissioner's Office (ICO).

3.4 This report has been structured based on the ICOs Data Protection and Audit Framework trackers which will be completed as part of the OPCCs assurance processes during 2026/27.

4. Accountability

4.1 The OPCC has a named DPO in place as is necessary under Article 37 of the UK GDPR. Further development and training opportunities across the OPCC are being identified to ensure the DPO is adequately supported to enable the role to be fulfilled as GDPR intends (i.e. to inform, advise, monitor compliance etc).

5. Data Sharing

5.1 Information sharing requirements for and with the OPCC is considered and assessed on a case-by-case basis taking into account legal requirements and policy.

5.2 During the reporting period there were two new areas of businesses where DPO advice was sought in relation to information sharing (this is consistent to previous years). In both cases a Data Protection Impact Assessment was undertaken which resulted in Information Sharing Agreements (ISAs) being created ensuring adherence to ICO best practice.

5.3 Lead Officers are advised to regularly review ISAs for their areas of businesses and where processes or requirements change continue to seek support and advice from the DPO.

6. Information and Cyber Security

6.1 The OPCC utilises the hardware/software and systems managed by Cleveland Police which ensures necessary technical, physical, personnel and procedural security controls to protect information held and accessed by the OPCC. This includes laptops, mobile phones, Microsoft Teams, access control etc.

7. Personal and Data Breach Management

7.1 During the reporting period, the OPCC assessed six potential data breaches (+2 compared to the previous year). The DPO was promptly advised of all possible breaches to enable a thorough assessment to take place. Following

assessment by the DPO, four of these incidents were confirmed as actual data breaches (consistent with previous year).

7.2 Of the four assessed breaches it was determined that none were likely to result in a risk to the rights and freedoms of the individuals concerned and therefore did not meet the criteria for reporting to the ICO within 72 hours.

7.3 As part of the local data breach assessment processes any opportunities for organisational learning are considered to prevent further breaches occurring. Any identified learning is shared direct with individuals involved in the data breach or across the wider team via email or team meetings as required.

8. Records Management

8.1 During the latter part of 2025/26 work commenced to understand the data and records currently held by the OPCC including where it is stored, how it is stored and whether it is being held and stored as per our data retention policy. This is a piece of work that will continue into 2026/27 and beyond to ensure adherence to our policy and in preparedness for the abolition of PCCs in May 2028.

9. Information Rights

9.1 Freedom of Information (FOI) Requests

During 2025/26 the OPCC handled fifty-seven FOI requests (+24 compared to the previous year) under the FOI act which can be broken down as below:

- 30 were responded to as an FOI by the OPCC (+12 compared to previous year)
- 26 received by the OPCC which were for the attention of Cleveland Police (+15 compared to previous year)
- 1 was a Subject Access Request (SAR) for the OPCC (+1 compared to the previous year)
- 0 SARs for Cleveland Police (-2 compared to the previous year)
- 0 were handled as case work (-2 compared to the previous year)

9.2 Of the fifty-seven requests the OPCC received five reviews (+4 compared to the previous year). FOI review processes are not mandatory but are seen as best practice by the ICO.

9.3 As members are aware for increased independence / quality assurance FOI reviews are considered by a member of the OPCC Senior Management Team (this will be the DPO moving forward) and presented to a small panel of Joint Audit Committee Members.

9.4 Of the five reviews there has been two occasions where recommendations have been made for the initial handling of the FOI to be reconsidered.

9.5 Furthermore, during the same period we have been made aware of six complaints to the ICO following our handling of FOI requests (+5 compared to the previous year). The status of these complaints are:

- 1 has been accepted as eligible for further consideration and remains open
- 2 have resulted in the issuing of a ICO decision notice
- 1 was withdrawn by the requestor
- 1 was investigated and resulted in no further action
- 1 resulted in a request for a more substantive response to be sent to the requestor prior to formal investigation

9.6 Subject Access Requests (SARs)

During 2025/26 the OPCC received five (+3 compared the previous year) SARs as below:

- 2 handled by the OPCC
- 1 handled by the OPCC but not completed due to ID not being provided by the requestor
- 2 directed to Cleveland Police

9.7 No other information rights requests were received during the reporting period.

10. Training and Awareness

10.1 All staff within in OPCC are required to complete annual data protection training via the Cleveland Police e-learning platform. During 2025/26 the team achieved a 100% compliance rate.

10.2 On 28th January 2026 the Data Protection Officer delivered a presentation to the OPCC team meeting providing a guide to the handling of personal data breaches.

10.3 Planned training for 2026/27:

- Certified DPO 4-day training (with exam) – May 2026
- Senior Responsible Owner Training for Chief Executive - June 2026
- FOI / Use of exemptions training 8th & 9th June 2026

11.0 Conclusion

11.1 The OPCC takes the handling of personal data extremely seriously ensuring Information Rights are handled efficiently and effectively as per UK GDPR and the Data Protection Act 2018.

11.2 Data Protection remains a risk on the OPCC risk register with mitigations in place to support management of the risk including annual e-learning training including ‘Managing Information’ and ‘Government Security Classification’

12. Implications

12.1 Finance

None arise

12.2 Diversity and Equal Opportunities

None arise.

12.3 Human Rights Act

The UK GDPR and Data Protection Act 2018 clearly sets of individuals rights in terms of Data Protection. Compliance with these are through the duties and responsibilities of the Data Protection Officer.

12.4 Sustainability

None arise.

12.5 Risk

Data Protection remains a risk on the OPCC Corporate Risk Register