Police and Crime Commissioner
CAMBRIDGESHIRE AND PETERBOROUGH
Darryl Preston

Office of the Police and Crime Commissioner
PO Box 688
PE29 9LA
Tel: 0300 333 3456
Email: cambs-pcc@cambs.police.uk
Twitter: @PCCCambs

FOI Response

Information provided under the Freedom of Information Act

Freedom of Information Request	
FOI Reference: FOI/OPCC/26-023	
Date of Request: 03/08/2026	**Date of Response:** 27/08/2026

Information Requested:

This is a request for recorded information under the Freedom of Information Act 2000.

It concerns complaint, complaint-review and related personal data processed by the Office of the Police and Crime Commissioner for Cambridgeshire and Peterborough from 1 February 2020 to 1 August 2026, or, if later, from the date on which the OPCC first commenced the relevant complaint-review or complaint-handling function.

The purpose is to establish how supposedly independent OPCC complaint material is hosted, segregated and protected within the Bedfordshire, Cambridgeshire and Hertfordshire collaborated environment.

Definitions

"Complaint material" includes complaints, reviews, dissatisfaction matters, evidence, correspondence, internal notes, draft findings, decisions, referrals, identity documents and related personal data.

"Police personnel" includes officers, employees, contractors, volunteers and collaborated personnel of Cambridgeshire Constabulary, Bedfordshire Police, Hertfordshire Constabulary and BCH shared services.

“Privileged access” includes system-administrator, database-administrator, service-desk, cybersecurity, backup, recovery, records-management, migration, support or equivalent technical access.

“Incident” includes suspected or confirmed unauthorised access, inappropriate browsing, excessive permissions, incorrect security-group membership, cross-force access, administrator access outside an authorised support task, accidental disclosure, loss, alteration, deletion, extraction, unavailable logs or any personal-data breach.

No credentials, network addresses, encryption keys or exploitable operational-security information are requested.

Information requested

1. Complaint systems

Please provide the name and general description of each electronic system, application, platform, tenant, database, document repository, shared drive, case-management system or email environment used to receive, store, search, review, transfer or retain complaint material.

For each system, identify:

a. the owner;

b. the host;

c. the operator or administrator;

d. whether the system is OPCC-specific or shared;

e. whether Cambridgeshire Constabulary, another BCH force or a collaborated unit administers it;

f. the information-asset owner; and

g. the system owner.

2. BCH infrastructure

Please provide recorded information stating:

a. whether OPCC complaint systems are hosted on Cambridgeshire Constabulary or BCH infrastructure;

b. whether the systems use a BCH-wide identity or account-management service;

c. whether users from more than one BCH force can be assigned permissions;

d. whether BCH ICT personnel administer the systems;

e. which force or collaborated body controls the relevant servers, cloud tenant, directory, application or database; and

f. whether any part of the infrastructure is hosted by Bedfordshire Police or Hertfordshire Constabulary.

3. Segregation

Please provide recorded information showing how OPCC complaint material is separated from:

a. Cambridgeshire Constabulary personnel;

b. PSD personnel;

c. the Chief Constable and Chief Officer Team;

d. Bedfordshire and Hertfordshire personnel;

e. BCH shared-service personnel without a business need; and

f. any person who is the subject of a complaint.

Please identify whether separation uses a distinct tenant, database, application instance, security domain, access group, folder structure or another technical control.

4. Ordinary access

Please provide:

a. the OPCC roles authorised to access complaint material;

b. all police, PSD, BCH or contractor roles authorised to access it;

c. the recorded access criteria;

d. the person or role approving access;

e. the organisation creating accounts and applying permissions;

f. the procedure for removing access;

g. the frequency of access reviews; and

h. the most recent completed access review.

5. Privileged access

Please provide recorded information identifying:

a. which organisations' personnel possess privileged technical access;

b. the categories of privileged role;

c. whether they can technically search, view, copy, export, restore, alter or delete OPCC complaint material;

d. whether they can add themselves or another user to an access group;

e. whether OPCC approval is required before access;

f. whether emergency or break-glass access exists;

g. whether administrator activity is logged; and

h. who independently reviews such activity.

6. Audit logs

Please identify whether the following are logged:

a. attempted and successful access;

b. searches;

c. opening or viewing records;

d. copying, downloading or exporting;

e. printing;

f. editing;

g. deletion;

h. permission changes; and

i. privileged administrator activity.

Please identify:

j. the log-retention period;

k. the organisation controlling the logs;

l. which organisation can alter or delete them;

m. who reviews them and how frequently; and

n. whether the OPCC can independently preserve and inspect them.

7. Independence safeguards

Please provide any recorded enhanced-security or conflict procedure applying where the complaint concerns:

a. the Chief Constable;

b. a Chief Officer;

c. Professional Standards;

d. Information Rights;

e. an ICT administrator;

f. a person capable of accessing the complaint system; or

g. alleged misuse of police information systems.

Please include any mechanism for restricting the case, monitoring access or moving it to an independently controlled environment.

8. Data-protection governance

Please provide:

a. the DPIA-screening record;

b. every draft or completed DPIA;

c. DPO advice and sign-off;

d. the ROPA entry;

e. the Article 9 assessment;

f. the Article 10 assessment;

g. the specific Schedule 1 condition assessment;

h. the Appropriate Policy Document;

i. every relevant Data Sharing Agreement;

j. any Article 26 arrangement;

k. any Article 28 agreement;

l. any controller-to-controller agreement;

m. every hosting or infrastructure agreement;

n. every relevant service-level agreement;

o. the access-control matrix;

p. the privileged-access policy;

q. the audit-log policy;

r. any security risk assessment;

s. any data-flow map; and

t. any audit, review or assurance report concerning the function.

For each record not disclosed, please state whether it is held, held in draft, held by another BCH body on behalf of the OPCC, withheld under an identified exemption or not held.

9. Security incidents and breaches

For the stated period, please provide annual totals for internally recorded incidents involving:

a. OPCC complaint material;

b. police or BCH personnel accessing or attempting to access OPCC material without a demonstrated need;

c. excessive or incorrect permissions;

d. privileged or administrator access;

e. cross-force access;

f. incorrect disclosure to Cambridgeshire Constabulary, PSD or another BCH force;

g. Article 9 data;

h. Article 10, allegation, victim or witness data;

i. identity documents;

j. missing, incomplete, overwritten or unavailable audit logs; and

k. inability to establish whether unauthorised access occurred.

For each category and year, provide:

1. incidents recorded internally;

2. incidents investigated;

3. incidents classified as personal-data breaches;

4. incidents reported to the ICO;

5. incidents not reported;

6. affected individuals notified; and

7. incidents resulting in disciplinary, technical, procedural or governance action.

10. ICO reporting

For each relevant ICO notification, please provide:

a. the date;

b. ICO reference;

c. incident category;

d. reporting controller; and

e. recorded outcome.

For incidents considered but not reported, please provide:

f. the recorded risk assessment or decision;

g. the role and organisation of the decision-maker;

h. whether the DPO was consulted; and

i. the recorded reason for non-notification.

Redacted or anonymised records are acceptable.

11. Shared-controller incidents

Please provide the recorded arrangement establishing:

a. which controller investigates incidents involving the OPCC and one or more BCH forces;

b. which controller decides whether an ICO report is required;

c. who informs affected individuals;

d. who preserves and supplies audit logs;

e. who investigates suspected access by police or BCH administrators; and

f. how disagreements are resolved.

Searches and information held on behalf of the OPCC

Please search beyond the FOI team, including:

• the DPO;

• complaints and review personnel;

• Cambridgeshire Constabulary ICT;

• BCH ICT;

• PSD;

• information security;

• legal services;

• records management;

• corporate governance;

• and relevant senior management.

Where a Constabulary or collaborated BCH unit holds information on behalf of the OPCC, please consider section 3(2) of FOIA.

Where another authority is said to hold information in its own right, please identify that authority and the recorded basis for that position.

OPCC Response:

It has been ascertained that the information you are requesting is not centrally recorded. In order to locate the information being requested it would require searching several document databases, spreadsheets or other collection of records and this will require numerous checks with various departments outside of our organisation to locate the individual/team that may hold the information that is relevant to your request.

Therefore, it is considered that the cost of complying with your request for information would exceed the appropriate limit of £450 as has been stated in the Freedom of Information (Fees & Appropriate Limit) Regulations 2004.

Section 12(1) of the Freedom of Information Act 2000 provides that –

"Section 1(1) does not oblige a public authority to comply with a request for information if the authority estimates that the cost of complying with the request would exceed the appropriate limit."

When refusing to provide an applicant with such information, because the cost of compliance exceeds the appropriate limit, section 17(5) of the Freedom of Information Act 2000 requires the OPCC to provide you with a notice which states that fact.

In accordance with the Freedom of Information Act 2000 this letter acts as a Refusal Notice under Section 12 of the Freedom of Information Act.

Under Section 16 advice and assistance, if you can narrow your request, we may be able to provide the data requested. As explained above, this request currently falls across many areas.