Audit and Risk Assurance Committee

Meeting Date	16 September 2026
Title	Annual information governance report 2025-26
Author(s)	Maxine Noel, Information Governance Manager
Executive Sponsor	Claire Amor, Executive Director of Corporate Affairs

Executive Summary

The annual information governance (IG) report is presented. The report covers the period April 2025 to 31 March 2026.

The total number of information requests continues to grow. With this, challenges to our refusal to provide information which the recipient is not entitled to, also increases via our internal review process.

An increase in the total number of data incidents. We record information incidents (and not just data breaches) and encourage staff to report all data incidents no matter how minor they may seem.

Appendices

1 – Annual information requests

2 – Annual information incidents

Action required	The Committee is asked to review the information provided and seek clarification on any areas.
Previous consideration	The report has been to ELT.
Next steps	Not applicable
Financial and resource implications	There is no direct financial impact
Associated strategic priority/priorities	Technology-enabled regulatory excellence and organisational sustainability

Associated strategic risk(s)	SR02 - Organisational Capacity
Risk appetite	Compliance - measured
Communication and engagement	Not applicable
Equality, diversity and inclusion (EDI) impact and Welsh language standards	Not applicable
Other impact assessments	Not applicable
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Audit and Risk Assurance Committee, 16 September 2026

Information Governance Annual Report - 1 April 2025 to 31 March 2026

Introduction

1.1 The Information Governance (IG) function within the Corporate Affairs directorate is responsible for the HCPC's ongoing compliance with the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and the Data (Use and Access) Act 2025. The Department also manages the HCPC's relationship with the Information Commissioner's Office (ICO), the information rights body.

1.2 Freedom of Information (FOI) and Environmental Information Regulations (EIR) legislation provide public access to information held by public authorities. Public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities. Both Acts contain defined exemptions to the right of access, which means that there are clear criteria on what information can and cannot be requested.

1.3 The DPA governs the protection of personal data in the UK. It also enables individuals to obtain their personal data from a data controller processing their data. This is called a subject access request. Data subjects also have certain other rights under data protection legislation. Namely:

- to be informed – the right to be informed about the collection and use of their personal data.
- to rectification – the right to have inaccurate personal data rectified or completed if it is incomplete.
- to erasure – the right to have personal data erased. The right is not absolute and only applies in certain circumstances.
- to restrict processing - the right to request the restriction or suppression of their personal data. The right is not absolute and only applies in certain circumstances.
- to data portability – the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- to object – the right to object to processing based on the legitimate interests or performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processes for the purposes of scientific/historical research and statistics.

- in relation to automated decision making and profiling – the right to be provided with information about automated individual decision-making including profiling.

1.4 This report provides an update on IG activity for the period 1 April 2025 to 31 March 2026.

Information requests

2.1 During the reporting period we received a total of 690 requests for information. This is an increase to the total of 564 information requests received in the previous reporting year. We have seen an annual increase in requests over the past few years; 26% increase in the last four years.

2.2 A total of 671 requests were closed in the reporting period. Of this, 53 requests were closed in breach of a statutory time limit for providing a response. This means that we responded to 92% of all requests for information within a statutory time limit.

2.3 The ICO self-assessment toolkit, which is designed to help public authorities assess their current FOI performance and provide indicators of where efforts should be focused in order to improve, categorises FOI response rates as follows:

Good	95% or more of FOI requests are responded to within the statutory timeframe.
Adequate	90%-95% of FOI requests are responded to within the statutory timeframe.
Unsatisfactory	Fewer than 90% of FOI requests are responded to within the statutory timeframe.

2.4 A breakdown of the annual figures can be found at Appendix 1.

Freedom of information (FOI) requests

2.5 In 2025-26 276 FOI requests were received (245 in 2024-25). The overall total number and complexity of FOI requests have increased. We have also noticed an increase in the use of AI in requests that have been received, which can lead to requests being more time consuming to read and understand.

2.6 Common FOI themes during the reporting period included allegation details of named Registrants subject to interim orders, requests for hearing transcripts, information about international registrants with breakdown by country of origin/training and breakdown of registrants with annotations. The launch of the data hub in May 2025 has seen a decrease in the number of routine FOI requests for top level statistics from the Register.

Subject access requests (SARs) and other data subject rights requests

2.7 In 2025-26 195 SAR requests were received (156 in 2024-25). SARs most often related to Fitness to Practise (FTP) cases. For example, a request from the complainant for a copy of the registrant's response to the matters raised in their complaint. We often receive widely scoped SARs for 'a copy of all personal data held' which requires a search of more than one system.

2.8 Details of the organisation's obligations for dealing with such requests is covered in the annual information security training.

2.9 Under Section 45 of the FOI Code of Practice 2018, it is good practice for organisations to conduct an internal review of an initial response where someone expresses dissatisfaction. The implementation of the Data (Use and Access) Act 2025 requires organisations to have a complaint handling process for handling complaints about how we've handled an individual rights request. We have always offered internal reviews as way of dealing with such complaints. We received 72 internal review requests (35 FOIs and 37 data subject rights requests were referred for internal review). This compares to 46 internal review requests received in the previous year. This 36% increase we believe is due to an increase in the overall number of FOI and data subject rights requests received.

Information incident management

3.1 The HCPC encourages an open incident reporting culture, with an emphasis on analysis and learning in order to identify any weaknesses in our processes and make appropriate changes.

3.2 Since February 2015, all incidents, regardless of how minor they may initially appear, are reported centrally and risk scored. A breakdown of the number of incidents that were reported can be found at Appendix 2.

3.3 In the reporting period, we recorded 107 information incidents. This is an increase to the total number of 86 incidents recorded for the previous year. We are unsure why there has been an increase in the number of reported incidents. However, it should be noted that we record information incidents (and not just data breaches). Some incidents were reported by data subjects but after investigation were assessed as being part of the usual regulatory process. We recently added this to the incident categories; since 1 March 2026, so that we now capture and record these.

3.4 The majority of incidents reported occurred in FTP followed by Registration. These areas of the organisation handle large volumes of personal data. Generally, most incidents are of the same common level of risk.

3.5 Human error related to not following processes was identified as the main cause of many incidents. Some weaknesses in systems and poor redaction were also highlighted.

3.6 Our analysis tries to identify the underlying cause of human error incidents. This can be found at Appendix D.

3.7 One of the recommendations from the BSI audit of ISO27001:2022 conducted in 2024 was that we should improve our ability to track and manage information incidents. Last year we reported to the Committee that we intended to make changes to the current IT Helpdesk system to incorporate logging of information incidents. However, we are unable to proceed with this as the IT Helpdesk software is unable to calculate the risk based on the criteria we use when assessing information incidents. Therefore, the idea of automating the process and sending out alerts to the team if close to a high risk would not be possible. The team is looking at alternative ways to automate the process and sending alerts for example using MS Forms.

3.8 One information incident was assessed as meeting the threshold for reporting to the ICO. It was closed by the ICO with no further action.

ICO Complaints and decisions

4.1 Part of the role of the Information Commissioner's Office (ICO) is to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public about information rights issues.

4.2 We received three complaints from the Information Commissioner as follows:

- The ICO contacted us to advise they had received a complaint that we had not responded to an FOI request despite the requester emailing us on three separate occasions. The ICO asked us to write to the requester and comply with the FOI request.
    - When investigating this matter, we discovered that the HCPC did not receive any of the requester's emails as they had been sent to an incorrect email address. The FOI request was for information not held by the HCPC.
    - ICO outcome: The ICO closed their case with no further action required by the HCPC.

- The ICO received a complaint from a data subject that we had failed to exercise their right to rectification/erasure. The ICO asked us to review the handling of the data subject's request.
    - Our investigation into this matter found that we had written to the data subject on three separate occasions to explain why we had to deny their request for erasure/rectification.
    - ICO outcome: The ICO was satisfied that we had complied with our statutory obligations and determined to close their case with no further action required by the HCPC.

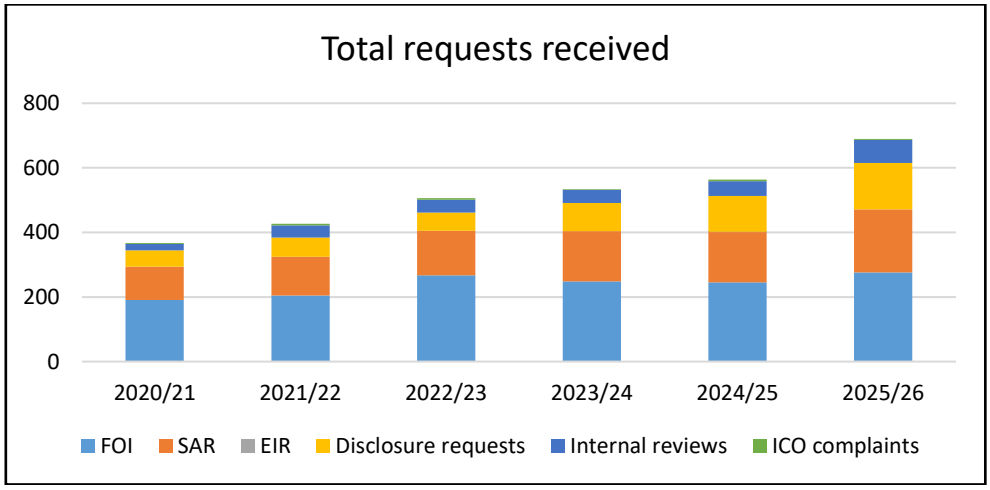
- The ICO received a complaint about our refusal to release information in response to an FOI request. The FOI request, from a member of the public, was for the qualifications of a Registrant.
    - ICO outcome: Awaiting further correspondence from the ICO regarding this matter.

Information Governance

5.1 During the reporting period the Information Governance team continued to develop and improve the information governance framework; the way we manage and dispose of information, identify and respond to data security incidents and ensure compliance with the FOIA and data protection laws.

5.2 Since January 2021, we have published on the HCPC website on a quarterly basis our FOI compliance statistics. It is good practice to publish these statistics as detailed in the Freedom of Information Code of Practice 2018, Section 8 Publication Schemes (paragraphs 8.5 and 8.6).

5.3 With the increasing workload within the team, we increased team resources by 0.5 full time equivalent (FTE). In September 2025, we recruited a Feedback and Information Officer role. This is a shared resource between the Information Governance team and the Feedback & Complaints team. There has been a period of time getting the role up to speed with the work undertaken by Information Governance, but they have proven themselves invaluable with assisting with the increasing number of information requests:



5.4 During the year, we updated our privacy notice. These changes include:

- splitting the Data Protection policy from the privacy notice. This was an agreed management action in the Data Protection internal audit (final report presented to this Committee at its March 2025 meeting);
- use of AI in plagiarism detection software; and
- adding a section on recorded telephone calls in the Registration department.

5.5 Data privacy impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project or new way of processing personal data. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. The team has advised, and assisted colleagues complete the screening questions and on those pieces of work requiring a full DPIA, as follows:

- Clobba call reporting
- Policy Consultation analysis NVIVO
- Workforce profiles I&A for web
- SolarWinds
- Keesing document verification
- IELTS
- e-Redact
- Generic AI web offerings
- NVIVO AI Analysis software
- Sanctions Policy Consultation
- Redactexpert (AI)
- Smartsurvey
- Partner Portal Data Migration
- WorkDay – Finance
- DD details transfer to BottomLine automation
- DocDefender
- Network Transformation Project
- FTP AI Risk Assessment
- Dogma BC Duplicates fix
- AI Generated Council-Comm minutes
- Try Booking
- ToC QA process
- Education OneDrive file sharing
- Doodle Pro
- Box
- DataFlow
- Customer Contact phase 2
- CoreHR-Access Group upgrade restart
- Test Of Competence video sharing
- TSG supporting BC via Softcat
- iBoss via Bytes
- ACOLAD Transcription
- NAO VALIDIS

5.6 We continue to review all our older MOUs. We have updated or newly signed a total of five MOUs as follows:

- NHS England
- Professional Standards Authority
- ACRO Police Records
- Health and Care Regulators draft NDA 4 IT
- DBS and Health and Care Professions Council

5.7 An MOU with The British Association of Sport Rehabilitators (BASRaT) is being prepared to allow that Voluntary Register to provide information that may be relevant to investigations concerning PH registrants, but HCPC will not share information with the professional body, under this agreement.

5.8 In March 2026, BSI undertook a three day audit of HCPC's ISO27001:2022 ISMS and supporting processes. No areas of non-conformance or areas for improvement were found. The full report was shared with this Committee in the June 2026 meeting.

5.10 All Information Security Management System (ISMS) documentation was updated by the ISMS Board over December 2025/January 2026. The ISMS Board has been updated to be the Information Security and Compliance Group, reporting to the Information and Technology Governance Board.

5.11 During the year, cyber security was subject to internal audit. The internal audit report was presented to this Committee at its meeting in November 2025.

5.12 Annual information security training is delivered to all staff (including contractors) as part of mandatory staff training. Partners and Council members are also asked to complete the training. At the time of writing, 91% of staff have completed this year’s information security training (excludes employees on long term sickness, maternity and sabbatical leave).

Decision

The Committee is requested to discuss the report.

Appendices

Appendix 1 – Annual information requests 2025/2026
Appendix 2 – Annual information incidents 2025/2026

Appendix 1 – Annual information requests

Table A - Breakdown of information requests received

	Q1	Q2	Q3	Q4	Total 2025/26	Total 2024/25
FOI	56	80	66	74	**276**	**245**
Data subject rights requests	41	64	48	42	**195**	**156**
EIR	0	0	0	0	**0**	**1**
Disclosure requests	28	37	36	43	**144**	**111**
Internal reviews	19	21	19	13	**72**	**46**
ICO complaints	0	1	1	1	**3**	**5**
Total requests received	**144**	**203**	**170**	**173**	**690**	**564**
Total closed	**138**	**187**	**201**	**145**	**671**	**523**
Response within statutory timescale	130	171	185	132	**618**	**497**
Response in breach of statutory timescale	8	16	16	13	**53**	**26**
% within statutory timescale	**94%**	**91%**	**92%**	**91%**	**92%**	**95%**

Appendix 2 – Annual information incidents

Table C- Data incidents quarterly breakdown

	Q1	Q2	Q3	Q4	Total 2025/26	Total 2024/25
No. of data incidents	23	38	22	24	**107**	**86**

Table D - Data incidents by category

Data incident categories - Total 2025/26												
CAUSE MATRIX	**Human Error**	**System/IT issue**	**Supplier Error**	**Process not followed**	**Process Weakness**	**Malicious Activity / Attempted Fraud**	**Paper Loss**	**Verbal Disclosure**	**Redaction failure**	**Internal Loss**	**Lack of suitable Training**	**Part of regulatory process**
Human Error		12	3	1					1			
System / IT Issue	6		1									
Supplier Error	7			1		3						
Process not Followed	41	1	1		2							
Process Weakness	7	2										
Malicious Activity / Attempted Fraud	1		2									
Paper Loss		1										
Verbal Disclosure												
Redaction failure	11		1									
Internal Loss							1					
Lack of suitable Training	1			1	1							
Part of regulatory process					1							1