Housing
Ombudsman Service

DATA PROTECTION ANNUAL REPORT 2024-2025

April 2025
Information Governance Team

Table of Contents

1. Introduction

This report summarises the Housing Ombudsman Service's (HOS) key activities in relation to information governance and compliance with relevant law, covering the period from 1 April 2024 to 31 March 2025.

The Housing Ombudsman Service is registered as a data controller with the Information Commissioner's Office. Our ICO registration number is Z5137330.

1.1 Data Protection in HOS

In August 2024, the existing Data and Digital Team was divided into two Information Governance Teams. The new teams are Information Governance Casework and Information Governance Compliance.

Along with the IT Support Team, these teams are now responsible for the Information Governance function in HOS. Information Governance is a broad term that encompasses data protection, information security, records management, and Freedom of Information.

These three teams, along with the Performance and Business Information team, comprise the Data, Digital, and Technology service, in the Finance and Corporate Services Directorate.

The Casework team is primarily responsible for data subjects' rights requests, Freedom of Information, data breach investigation, and records management. The Compliance team is primarily responsible for advising on data protection matters, training, organisational security measures, and other compliance activities. The Compliance Manager is also the designated Data Protection Officer under Article 37 of the UK GDPR.

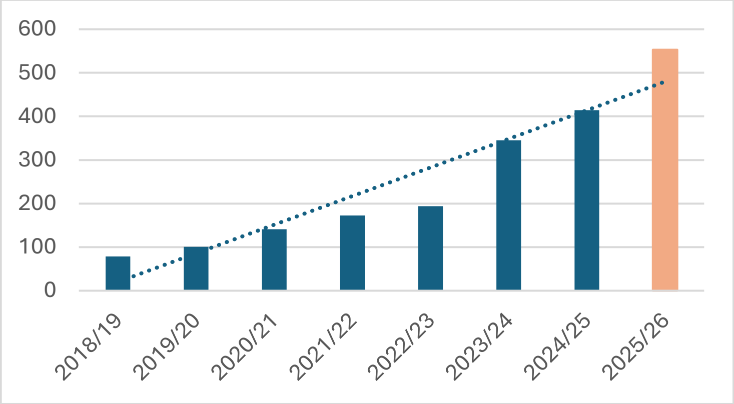
2. Data subjects’ rights requests

2.1 Right of Access (Subject Access) Requests

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information about the processing of that data. It helps individuals to understand how and why an organisation is using their data and check they are doing it lawfully.

In the 24-25 financial year, HOS received 414 subject access requests. This is an increase of 69 (20%) from the previous year. The steadily increasing demand in cases is easily seen by the trend line in the chart below.

	SAR received	Percentage increase
2018/19	79	
2019/20	101	27.85%
2020/21	141	39.60%
2021/22	173	22.70%
2022/23	194	12.14%
2023/24	345	77.84%
2024/25	414	20.00%
2025/26	553	33.35%



The figures for the 2025/26 year are based on a prediction that requests will increase by 33.35%, the average annual increase since records began in 2018/19.

The prediction of future figures does not take into account any major changes in HOS business such as the possible addition of Private Rental Sector (PRS). There is potential for additional SAR from PRS tenants, and also potentially SAR from landlords. While our current landlords’ staff members have the right to make SARs, it is rare for them to do so. PRS landlords may be sole traders, or otherwise comprised of individuals who are more likely to exercise this right with HOS.

It is expected that PRS will add to the SAR caseload at least a similar request per resident ratio as the existing scheme. In addition, the inclusion of Social Tenant Access to Information Scheme in the Housing Ombudsman Scheme will create additional casework for HOS along with associated requests for information. Future planning for the Information Governance service will need to take this into account.

2.1.1 SAR Performance

In 2024-25, 407 SARs were closed. Of these, 379 were responded to on time within the requirements of the UK GDPR – normally one calendar month. This gives us a compliance rate of 93%. The Information Commissioner’s Office (ICO) rates this performance as “adequate”.

Period	Compliance %	ICO Performance Rating
18/19	78.50%	Unsatisfactory
19/20	68.30%	Unsatisfactory
20/21	87.20%	Unsatisfactory
21/22	95.40%	Good
22/23	95.80%	Good
23/24	97.00%	Good
24/25	93.12%	Adequate

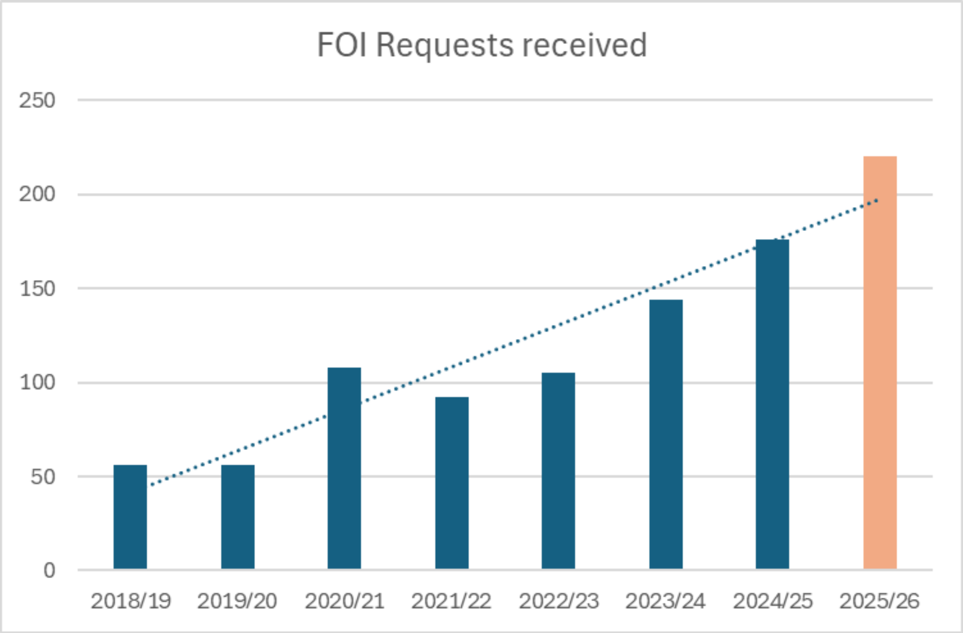
Good	95% or more of requests are responded to within statutory deadline
Adequate	90 to 95% of requests are responded to within statutory deadline
Unsatisfactory	Fewer than 90% of requests are responded to within statutory deadline

2024/25 has been a challenging year for the IG team with changing personnel and a restructure amid the increasing demand. The IG Casework team has done well to maintain an adequate level of performance under highly challenging circumstances which has seen the team not being at full resource capacity until early 2025.

2.2 Freedom of Information (FOI) Requests

The Freedom of Information Act 2000 provides public access to information held by public authorities. HOS has been a public authority for the purposes of the Act since we were added to Schedule 1 of the Act in 2018. We have observed a steadily increasing number of requests over that time, similar to the increases in SAR.

Period	FOI Requests received	Percentage increase
2018/19	56	
2019/20	56	0.00%
2020/21	108	92.86%
2021/22	92	-14.81%
2022/23	105	14.13%
2023/24	144	37.14%
2024/25	176	22.22%
2025/26	220	25.26%



Last year’s annual report predicted 168 requests and the final figure was 176.

The predicted figure for 2025/26 is based on an average annual growth rate of 25.26% since records began, shown by the trend line. We anticipate 220 requests for the coming year.

It should be noted that numbers of FOI requests received by an authority are roughly proportionate to the interest shown by the public – the more high profile an organisation is, and the more prominently it features in news articles, the more requests for information it receives. Any major publicity campaigns or high profile changes to the Scheme like the addition of PRS are likely to increase the number of requests we receive significantly.

2.2.1 Freedom of Information Performance

Of 175 cases closed in 2024/25, 164 were closed within the timescales required by legislation (normally 20 working days from receipt). HOS compliance for the year was 94%. This is a reduction since the previous year but still a solid result given the resourcing issues experienced by the team and is rated “adequate” by the ICO.

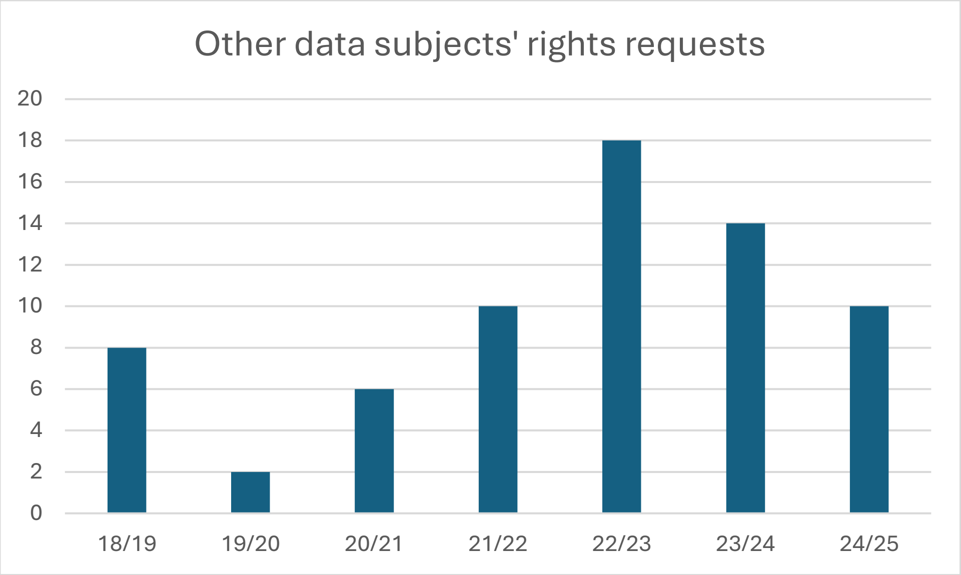
Period	Compliance %	ICO Performance Rating
18/19	89.30%	Unsatisfactory
19/20	89.50%	Unsatisfactory
20/21	88.90%	Unsatisfactory
21/22	100.00%	Good
22/23	100.00%	Good
23/24	97.20%	Good
24/25	93.71%	Adequate

2.3 Other data subjects’ rights requests

As well as the right of access, the UK GDPR allows data subjects other rights over their personal data held by organisations. The most commonly exercised of these within HOS are the rights to:

- rectification e.g. having incorrect data corrected or incomplete data completed
- erasure e.g. having data removed
- restrict processing e.g. requesting that data not be processed in specific ways
- object e.g. requesting that data is not processed at all

Generally, HOS receives very few subject rights requests other than those relating to the right of access. In 24-25, HOS processed 10 such requests. When compared to previous years, no clear trend can be predicted with confidence, and the low numbers are not anticipated to significantly impact on resources when compared to other cases.



3. Personal data breaches, near misses and security incidents

A personal data breach is defined as ‘a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.’

HOS sets a very low threshold for classifying something as a data breach. We require staff to report any incidents detected regardless of severity. This is helpful intelligence in identifying where we may have systemic weaknesses in systems or procedures, resulting in frequent reports of low severity breaches, and it should be noted that this may be helpful to identify risks of more significant breaches.

However, such a low threshold results in high numbers of reports. Such numbers of data breaches should not be regarded as an indicator that personal data is at risk. Nearly all of these incidents are extremely unlikely to result in any detriment to the individuals concerned.

3.1 Incidents reported

In 24-25, there were 385 reports of data breaches for the Information Governance team to investigate. This is an increase of 51.92% from the previous year. Given the increased headcount of staff and ever-increasing number of cases being handled by HOS, an increase in the overall number is to be expected.

Most common types of breach report:

Unauthorised disclosure - email	166
Landlord or external party breach	60
Data stored incorrectly [redacted]	34

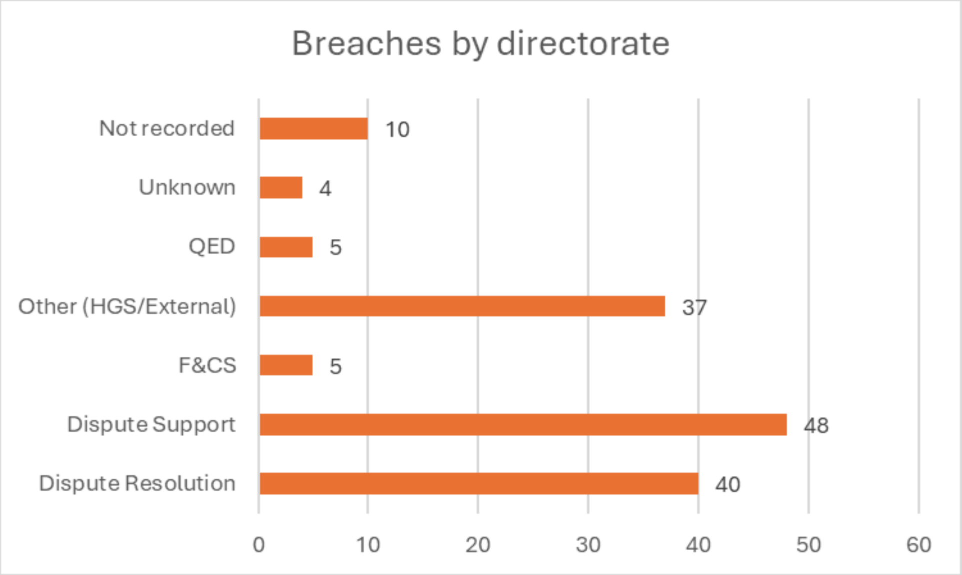
To establish a better comparison to indicate a trend, the number of reports has been compared against the average number of staff for the year. The table below shows the number of reports per 100 staff for the last three years. The actual increase when measured against staff numbers can be seen.

Year	Reports	Average headcount	Reports per 100 staff	Adjusted change in report numbers
2022/23	115	187	61.5	
2023/24	260	370	70.3	14.3%
2024/25	385	452	85.2	17.5%

On investigation, only 149 of the 385 reports were found to be actual breaches and attributable to HOS.

Year	Confirmed breaches	Average Headcount	Breaches per 100 staff	Adjusted change in breach numbers
2022/23	Not reported	187		
2023/24	101	370	27.3	
2024/25	149	452	33	20.80%

Of the 149 confirmed breaches, 133 were given the lowest risk rating, 14 are still under investigation and are as yet unscored. Two incidents were scored as medium risk.



The higher number of breaches seen relating to Dispute Support and HGS reflects the fact that this is where the errors are most likely to happen – these are the people interacting with residents and landlords most frequently and making the initial records where errors can lead to breaches.

3.2 Reporting delay

The sooner an incident is detected and managed, the less likely it is to result in harm to the data subject(s) involved.

In 2023-24, the average time between occurrence and reporting was 64 days. This year, the average time was 62 days. These high numbers are primarily due to a small number of cases remaining undetected for periods of more than a year before being noticed. There were 31 cases with a delay of 100 days or longer, down from 50 in 2023-24.

Delays in identifying breaches are closely linked to delays between cases receiving attention from caseworkers – often the breach will go undetected while a case waits in a queue. Improved case handling times in Dispute Resolution is also likely to result in a reduction in reporting delay for data breaches.

3.3 Breach notification to Information Commissioners Office (ICO)

There were no notifications made to the ICO this period in respect of data breaches reported.

3.4 Breach Tolerance Levels

The October 2022 internal audit on GDPR and Cyber Security recommended that "management should set the parameters for the frequency and severity of breaches that are tolerable, so that evaluation of monthly MI will allow assessment of the effectiveness of efforts to secure information assets that IAO's are responsible for."

Consequently, targets were set to reduce the most common breach type of "unauthorised or erroneous disclosure of personal data by email" by 10%.

Breach Incident Type	**2023-24**	**Target for 2024-25**	**Actual 2024-25**
Unauthorised or erroneous disclosure of personal data by email	79	87	114
Rate per 100 staff	21.4	19.2	25.2

The target has not been met.

Unauthorised disclosure by email most commonly means that the wrong landlord has been identified when a case is recorded, leading to case details being sent to the wrong landlord. Sometimes, it is due to the resident's email being recorded incorrectly. The data in question is almost always in relation to a single subject and there is minimal risk to the subject.

While this may be a useful indicator of weaknesses at the point of data entry, these "breaches" should not be viewed as resident data being at risk on a significant scale. It is not a good indicator of the overall security of the asset and HOS should look into a different way of tracking security and the risk of data breaches likely to cause actual harm.

Nevertheless, the DPO recommends this data should continue to be monitored and reported on as it is useful for highlighting weaknesses in records management.

4. Training and awareness

The Information Security and Data Protection policies set requirements for staff training and awareness in HOS.

All staff are required to undergo the Civil Service Data Protection and Cyber Security e-learning training when they start work with HOS. They are required to complete this training annually.

All staff are then required to attend a data protection and information security induction that is run at least once per month by the IG Compliance Team.

Staff are required to complete a refresher training session once every two years.

4.1 Training records [Section removed for publication]

4.2 New starter induction sessions:

It is best practice to ensure that all staff receive data protection and information security training when they start work for the organisation. We do this with an in-person session run [redacted] by the Information Governance Compliance Team on a monthly basis and all new starters receive the invite as part of their induction.

There were 106 new starters between 1 April 2024 and 31 March 2025. Of these, only 1 has not completed the induction training. This person is enrolled to take the course in May 2025.

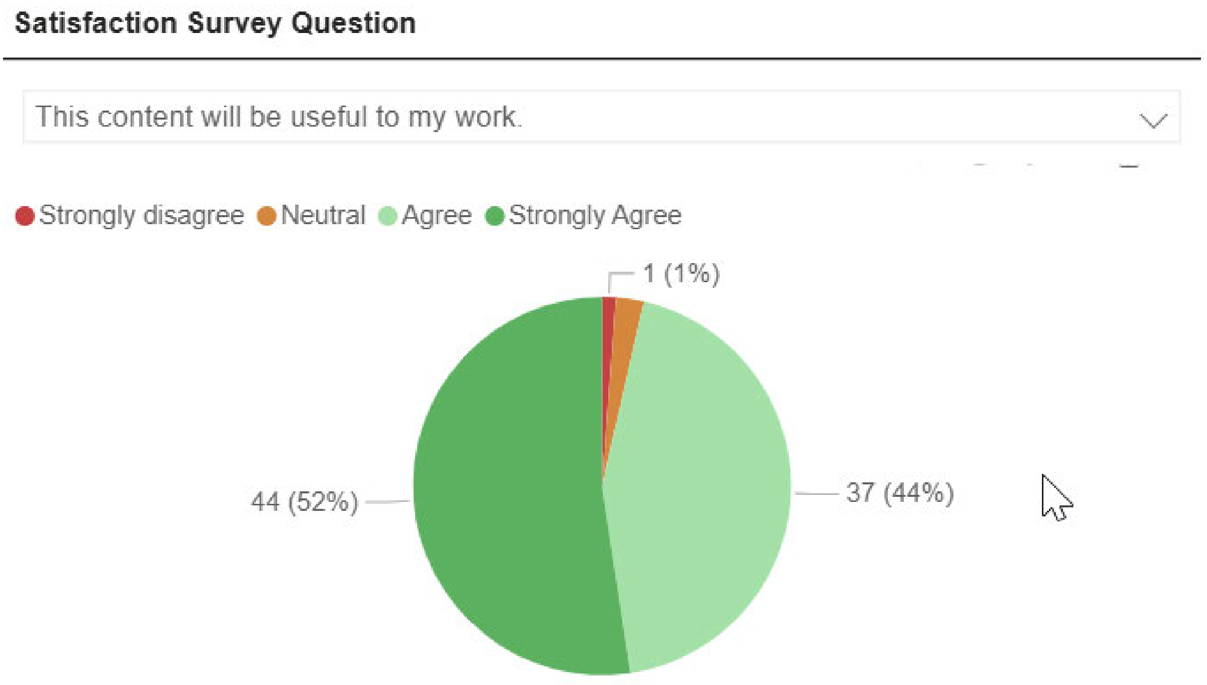
4.3 Refresher training

In January 2025 the Compliance team launched a new refresher training through [redacted]. It is a series of short video modules between 10-15 minutes each, designed to allow users to complete in their own time and around other tasks.

The videos are recorded specifically for HOS, delivered and tracked through [redacted]

97 staff have completed the new Data Protection and Information Security refresher training since it was launched on 27 January 2025. 95 staff completed the previous in-person induction and refresher training between October 2023 and 27 January 2025.

It has been well received, with 85% of learners completing the satisfaction survey, and of those, 96% agreed when asked if it will be useful to their work.



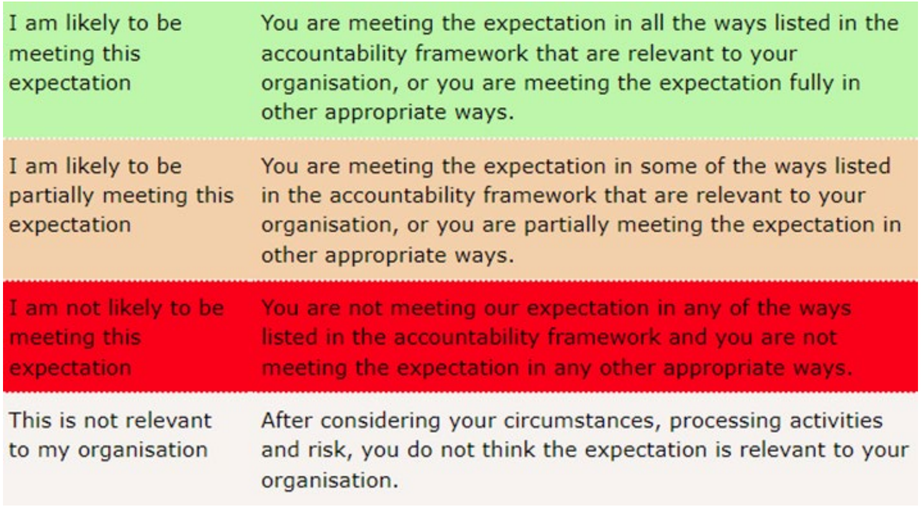
Satisfaction Survey Question

This content will be useful to my work.

5. ICO accountability framework self-assessment

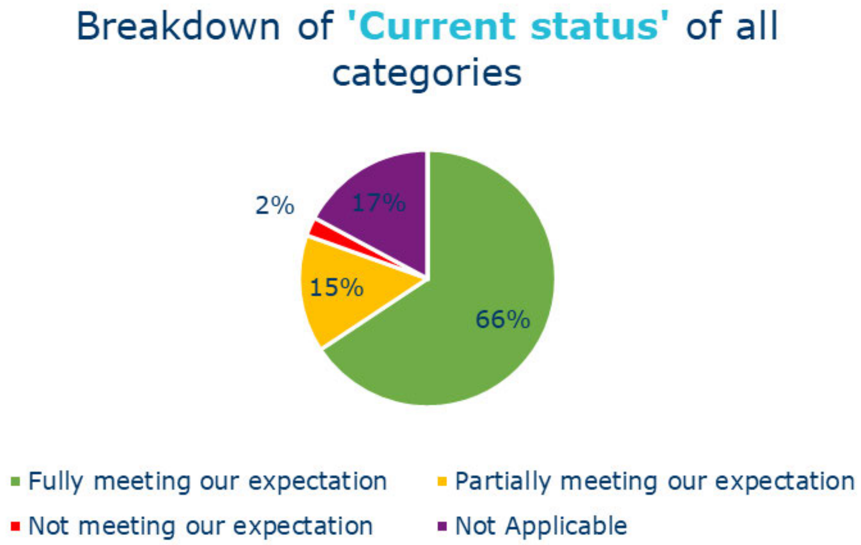
The ICO accountability framework self-assessment tool is a means by which an organisation can assess the extent to which they are currently meeting the ICO's expectations in relation to the accountability principle.

The assessment presents a series of statements that reflect the ICO's expectations of a data controller in terms of meeting the accountability obligation under the UK GDPR. The organisation is asked to rate how well they are meeting that expectation as below:



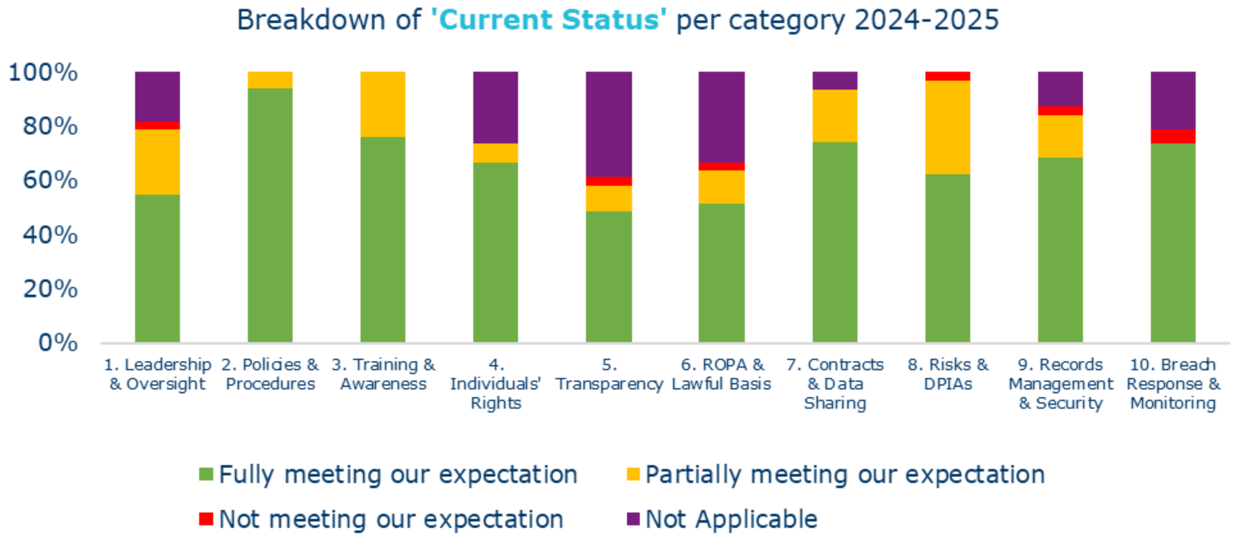
I am likely to be meeting this expectation	You are meeting the expectation in all the ways listed in the accountability framework that are relevant to your organisation, or you are meeting the expectation fully in other appropriate ways.
I am likely to be partially meeting this expectation	You are meeting the expectation in some of the ways listed in the accountability framework that are relevant to your organisation, or you are partially meeting the expectation in other appropriate ways.
I am not likely to be meeting this expectation	You are not meeting our expectation in any of the ways listed in the accountability framework and you are not meeting the expectation in any other appropriate ways.
This is not relevant to my organisation	After considering your circumstances, processing activities and risk, you do not think the expectation is relevant to your organisation.

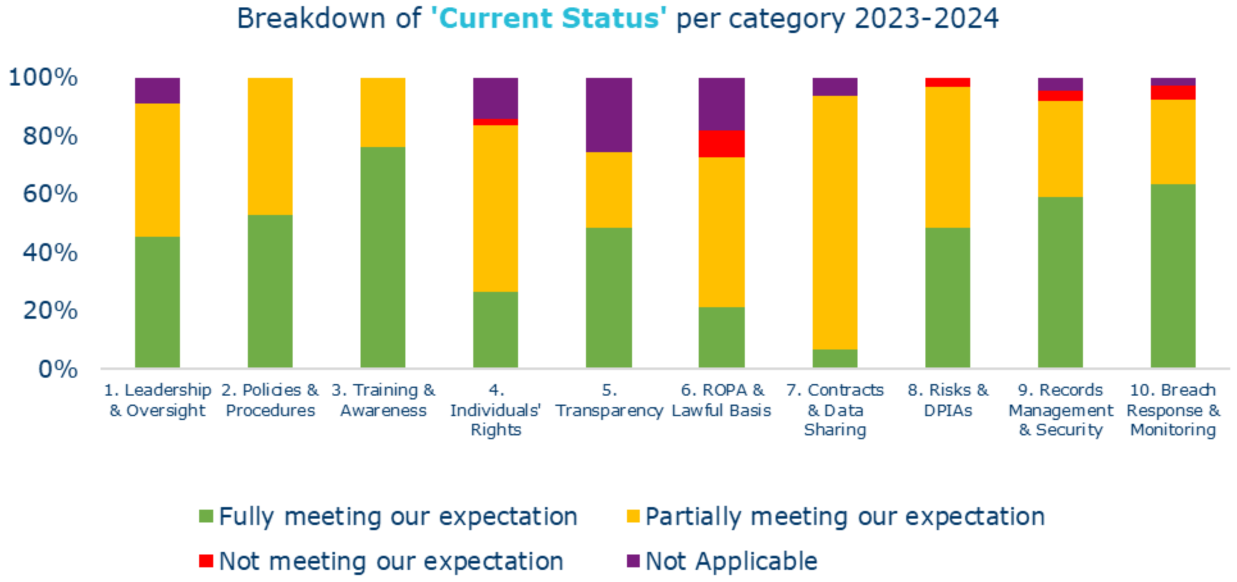
This self-assessment is completed annually by the Data protection Officer (DPO) in order to gauge improvements in HOS' overall privacy compliance. The full self-assessment is available to view at appendix B. Below is a summary of the self-assessment category breakdowns recorded:



This data shows that 66% of the self-assessment statements were assessed as “Fully meeting our expectation”. This is an improvement over the previously year’s 44%, and reflects large improvements in the sections of:

- Policy and Procedures – includes the new Information Security and Information Rights Policies
- Individual Rights – improvements in process and reporting have been made, and now that the team is back at full strength after some resourcing and staff absence issues, confidence is high that the team is now in a good position to manage the future caseload.





The self-assessment has identified the following key areas for improvement:

1) Continuing to develop the Information Asset Register and the uses of it will directly improve our compliance in a number of areas:

   5. Transparency
   6. ROPA & Lawful Basis
   7. Contracts and Data Sharing
   8. Risks and DPIA
   9. Records Management and Security

The asset register development is discussed further in section 6.1.1

2) The DPIA procedure will be reviewed and is likely to result in better compliance with section: 8. Risks and DPIA.

3) A review of KPIs in relation to records management, data protection, and information security, and how they are reported and monitored through the Information Governance Steering Group is likely to improve our compliance with sections:

   1. Leadership and Oversight
   9. Records Management
   10. Breach response and monitoring

6. Priority workstreams in 24-25

6.1. Information Governance Team projects

In 23-24 we identified the following activities to prioritise, through the self-assessment and GIAA audit:

- Information Asset Register
- Contracts and supplier data protection and security due diligence

6.1.1 Information Asset Register

The Information Asset Register is a foundational requirement for good Information Governance. It is a large undertaking for any organisation to create such a register, but the benefits are significant.

The IAR is a central record of all HOS information assets, giving enhanced visibility of our assets and accountability for those assets, making it easier to manage and protect them. When fully developed, it will improve risk management, identifying critical systems and helping with prioritisation of security and disaster recovery testing. It will demonstrate compliance at a glance and the HOS register includes the required Records of Processing Activities mandated by Article 30 of the UKGDPR.

The register was created and populated with critical assets in Q4 2024-25, and all assets have been scored for business criticality as recommended by the 2022 GIAA audit.

In 2025 we intend to link the assets in the register with related contracts and supplier management reviews, risk registers, and further compliance activity such as linking assets that process special categories of personal data to required ‘appropriate policy documents’. The aim is to provide a single place where one can review all of the key information relating to all information of value held by HOS.

6.1.2 Contracts and supplier data protection and security due diligence

We intend to implement a consistent process for evaluating suppliers in terms of data protection and security, ensuring that all contracts and agreements are in place and contain the appropriate clauses, and that our suppliers have adequate assurance measures in place.

This work is currently done but will benefit from standardisation and clear guidance on how to evaluate suppliers and their documentation.

Due to resourcing shortages this work has had to be deferred until 2025-26.

6.2 Policy Framework

Strengthening the policy framework around data protection and data security has been one of the priorities for the DPO. As noted in the ICO’s accountability tracker, HOS has greatly improved in this area (Section 5)

The main priority for 2024-25 was the Information Security Policy, which is now in place. In addition, the Data Subjects' Rights policy was also delivered.

6.2.1 Information Security Policy

An Information Security Policy is a requirement for many assessment frameworks and certifications. For HOS, it was also a chance to formalise and put into policy a lot of things we already practiced, and make our expectations in this area clear to all stakeholders.

The policy acts as an umbrella policy, referring to a number of sub-policies such as the IT Acceptable Use Policy and the upcoming Employee Monitoring Policy.

The policy sets out roles and responsibilities, sets standards for suppliers to meet, describes how we will implement new systems, hardware and software, and sets out how we will handle security incidents, among a number of security measures.

The policy was drafted in Q3 and approved by ELT in Q4.

6.2.2 Data Subject Rights Policy

Chapter 3 of the UK GDPR sets out the rights that an individual has when it comes to their own personal data. These rights include Subject Access, the right to rectification, the right to object, and the right to erasure. Our policy now sets out how HOS will approach requests to exercise these rights.

6.2.3 Policies in development for 2025-26

In 2025-26, the Information Governance Teams will be aiming to deliver policies governing:

- Employee Monitoring
- Records Management including Retention and Disposal

7 Data Protection Impact Assessments (DPIAs)

A DPIA is a tool that helps an organisation understand the processing of personal data that it does, or plans to do, in relation to a specific activity. As part of the DPIA process, we will describe the activity and all the ways personal data will be processed. We will assess the activity against compliance with data protection legislation, and we will look to identify any risks to the data subjects associated with the processing.

DPIA are mandatory when high risk processing is being carried out or certain types of activities are being proposed that may impact on the rights and freedoms of individuals, such as mass surveillance and profiling.

HOS uses a DPIA screening form where staff proposing new data processing related activities, such as projects, acquiring new tools and software, or new policies, are required to notify the DPO. This includes when significant changes are being made to these activities.

In 2024-25, 48 screening forms were submitted to the Compliance team. None of the forms indicated any mandatory DPIA were required. 11 full DPIA were conducted on a discretionary basis.

No DPIA in this period have identified any residual risks requiring sign-off by the Senior Information Risk Owner (SIRO).

8 Information Security

The responsibility for Information Security is split between the Information Governance Manager (Compliance) and the IT Manager.

Information Security is often viewed as having two main components; technical and organisational. The IT Manager is responsible for technical measures, such as properly configuring hardware, software, and monitoring security systems. The Compliance team is responsible for training the organisation, raising awareness and embedding good security culture.

Both parts are essential to good information security. The best designed and maintained technology in the world cannot deliver good security if the people using it do not value and understand the security measures and their role in security.

8.1 IT Estate

The managed IT estate has grown from 425 devices and 16 Mobile phones in 23-24 to 530 laptops and 37 mobile phones at the end of 24-25.

[redacted]

To ensure robust cybersecurity, we conduct regular penetration testing and continuous monitoring. Internally, we perform two comprehensive penetration tests annually, alongside an external penetration test conducted once per year. These tests simulate real-world attacks to identify and remediate vulnerabilities before they can be exploited. In addition, we run daily automated vulnerability scans across our infrastructure, enabling rapid detection and response to emerging threats. We also benefit from external threat monitoring provided by the UK’s National Cyber Security Centre (NCSC), which enhances our situational awareness and supports our proactive security posture.

8.2 [removed for publication]

8.3 [removed for publication]

8.4 Security incidents of note

One of the measures implemented in 2024-25 and formalised in the Information Security Policy is the Incident Response Team (IRT). The IRT is made up of members of the IG Compliance and IT Teams, and governed by a terms of reference.

The purpose of the IRT is to be the first response when an incident is detected and to triage the incident, assessing risks and escalating decisions as required. The IRT is activated whenever one of the members is alerted to an incident that requires an immediate response.

In 2024 the IRT was activated four times for notable security incidents:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

The IRT reports risks and learning from incidents to the SIRO.

8.5 Defending against Phishing attacks

Phishing remains one of the most common methods of cyber attack. Attackers send large numbers of emails containing malware, or links to unsafe sites, and hope that a few people will take this ‘bait’. A successful attack can result in malware being installed on a user’s device or authentication credentials such as usernames and passwords being obtained by the attackers.

[redacted]

[redacted]

[redacted]

8.5.1 Campaign results

HOS runs regular “Phishing campaigns” to maintain awareness, with the goal being to get our people to “think before you click”. In 2024-25, we sent a total of 2,583 test emails that were received by staff.

[Paragraphs have been removed from this section for publication]

8.6 Security Assessment Proficiency Assessment (SAPA)

The Security Awareness Proficiency Assessment (SAPA), [redacted] seeks to assess HOS’ susceptibility to cyber attacks by scoring users across seven knowledge areas which include:

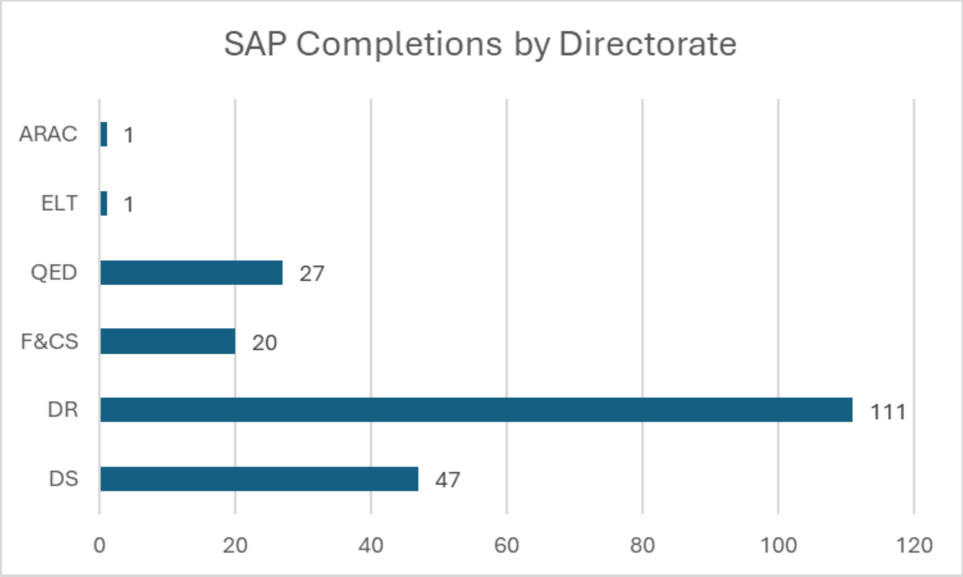
- Email Security
- Incident Reporting
- Internet Use
- Mobile Devices
- Passwords and Authentication
- Security Awareness
- Social Media Use

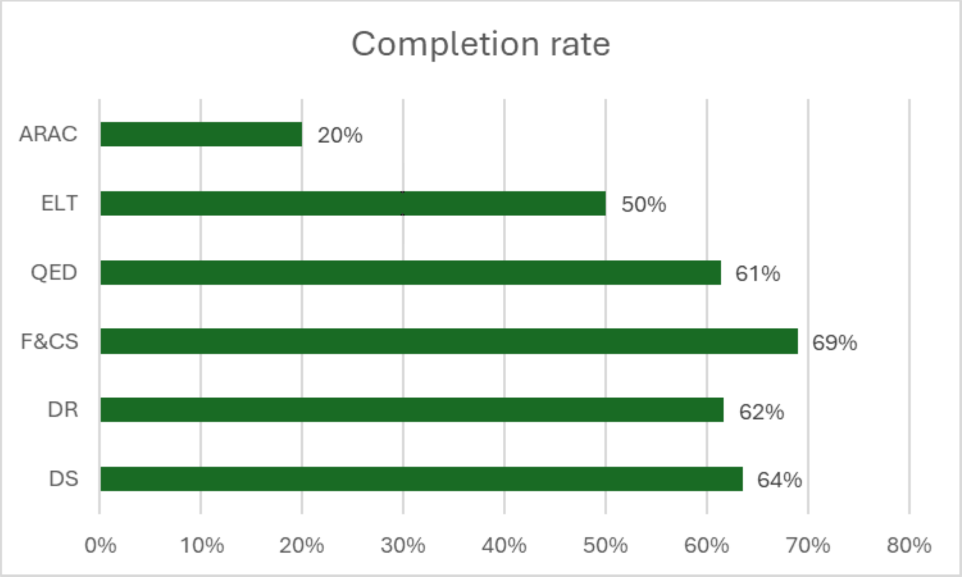
This assessment is sent to all colleagues annually for completion. It is useful data to indicate where our efforts to educate and raise awareness may be required and where we already have strong security awareness.

334 staff were sent the survey and 207 (62%) completed it.

Department	Completed	Enrolled	Completion rate
ARAC	1	5	20%
Dispute Resolution	111	180	62%
Dispute Support	47	74	64%
Executive Leadership Team	1	1	100%
Finance & Corporate Services	20	29	69%
QED	27	44	61%
Grand Total	**207**	**334**	**62%**

In 2025-26 the survey will be mandatory and we will be following up non-completion with line managers.





9. Future projects and service improvements

9.1 Information Asset Register

The Information Asset Register requires further development. In 2025-26, we aim to finish populating the register, get the entries into a regular review cycle, and then expand our use of it, linking our connected compliance activities for the assets such as policies, contracts and supplier due diligence and risk management.

This will further enhance our ability to view our information assets and demonstrate accountability for our information.

9.2 AI and Copilot.

Artificial Intelligence technology presents opportunities for HOS and we intend to make good use of the technology.

We have started a Data Protection Impact Assessment and a trial of Co-pilot in the Corporate Governance team. Co-pilot is an AI system that is already heavily tested and used in central government and respected agencies including the Information Commissioner's Office.

Future Co-Pilot or other AI procurement and deployment will require a process of evaluation and testing which will be conducted through the AI working / Information Governance Steering Group as part of the standard procurement processes.

We intend to introduce Co-pilot slowly, beginning with low-risk activities such as meeting management. This is now in trial with the Corporate Governance team. Their work is best suited to an initial trial – the team is small, but the work is heavily focused on time consuming tasks related to lengthy meetings that co-pilot is well suited to help with – automatic summaries of decisions and actions, and generating minutes. We intend to gradually expand our use of AI, working to improve how our data and systems are structured, classified, and labelled to optimize our data environment.

We will continue to develop our understanding of AI and our strategy towards using it for our work in HOS.

10. Conclusion

In 2024-25 HOS has continued to develop our data protection and security functions and we have made significant successful progress. There are a number of challenges on the horizon and the Data, Digital and Technology service will need to continue to adapt and develop our capabilities in order to meet them.