# The ICO at a turning point: what its final Annual Report reveals




**Daniel Bishop**
Associate

**Alison Llewellyn**
Senior Knowledge Lawyer

**Katie Hewson**
Partner and Head of Data Protection

**Sarah O'Brien**
Partner

Stephenson Harwood

*Daniel Bishop, Associate, Alison Llewellyn, Senior Knowledge Lawyer, Katie Hewson, Partner and Head of Data Protection, and Sarah O'Brien, Partner, all at Stephenson Harwood, examine what the ICO's 2025/26 Annual Report reveals about its evolving regulatory and enforcement priorities, and the practical implications for organisations and DPOs as the regulator transitions to the new Information Commission.*

The Information Commissioner's Office ('ICO') has published what it has stated publicly to be the last full annual report ('Report') in its current form, before the corporation sole model is replaced by the board-governed Information Commission introduced by the Data (Use and Access) Act 2025 ('DUAA').

The Report has been published at an undeniably turbulent time for the ICO, landing shortly before the Department for Science, Innovation and Technology ('DSIT') announced seven non-executive appointments to the regulator's new board. DSIT itself was abolished less than a week later by the new Burnham administration. Deputy Commissioner and Chief Executive Paul Arnold remains temporarily responsible for the Information Commissioner's responsibilities, following John Edwards' resignation in June 2026 amid an independent workplace investigation. A review of the ICO's culture, accountability and governance also remains ongoing and will now sit with the Department for Digital, Culture, Media and Sport, which assumes responsibility for the regulator as its sponsoring department. The Foreword from Paul Arnold suggests the Report marks an important ending and critical new beginning for the regulator. It makes a clear statement as to the regulator's thoughts on harm, proportionality and its own leverage, and looks ahead to where enforcement pressure will likely fall over the next 12 to 24 months. With complaint volumes placing unprecedented pressure on the regulator, the incoming Information Commission stands to inherit both a sharper enforcement pipeline and a serious capacity issue.

In this article, we offer a practitioner's read of the report, considering what the ICO's direction of travel now looks like; what the enforcement trends tell us about compliance risk; what the governance disruption implies for accountability inside supervised organisations; and what should sit near the top of the Data Protection Officer's ('DPO's') agenda between now and the end of 2026/27.

## A regulator in transition

The imminent abolition of the ICO as a corporation sole and the establishment of the Information Commission as a body corporate is expected to modernise the way in which data protection is regulated and enforced in the UK. The Information Commission will be governed by a Chair, a Chief Executive and non-executive directors appointed by the Secretary of State.

The Report presents this new governance structure as a means of improving resilience, strategic leadership, and

accountability. The events surrounding the resignation of John Edwards provide immediate context for this, but the implications go much further. The structure of the regulator can also shape the regulatory landscape with the potential to alter how priorities are set, engagement with relevant stakeholders, and prioritisation of enforcement action.

## Impact-based regulation

One of the clearest themes running through the Report is the ICO's continued focus on impact-based regulation. The Report repeatedly seeks to emphasise that successful regulatory outcomes cannot be measured by the volume of investigations opened or fines issued. Instead, the regulator's focus is on achieving behavioural change and preventing harm before it can occur.

The Report also describes how the ICO has undergone a 'critical' transformation programme with a view to modernising its approach to regulatory interventions. This transformation is said to have led to more focused, impactful enforcement actions, with a greater emphasis on proportionality and measurable outcomes. However, this should be seen in the context of a regulator that only progressed 2% of personal data breach reports to a formal investigation in the year 2025/26. The overwhelming majority of reports (91%) were closed with only informal (advisory) action having been taken. The remaining 7% were closed with no further action taken.

For organisations, this may provide a degree of comfort as it signals a regulator continuing to prioritise remediation and prevention over hard-line enforcement action. It is also a sign that engaging in an open dialogue with the regulator when things go wrong will not necessarily lead to heavy enforcement action (or any enforcement at all). Provided that the reporting organisation is cooperative and commits to improving its compliance posture, the figures show that the regulator is much more likely to take informal (advisory) action (if it takes any action at all), saving formal enforcement action only for the most egregious compliance failings.

The best mitigation for organisations in the face of a regulatory investigation is to ensure any investigations, remedial action and lessons learned are effectively documented, implemented and monitored in accordance with a robust data breach response plan. This will demonstrate to the regulator that the organisation is well-equipped to discharge its regulatory obligations and that it takes these seriously. In those circumstances, the organisation will have signalled to the regulator that no regulatory enforcement action is required to invoke positive behavioural change.

## Enforcement trends

Throughout the year 2025/26, the ICO issued a series of high-profile fines, including a £14.47 million fine to Reddit for failures around children's data, and £14 million to Capita in relation to a personal data breach arising from a cyber-attack. There were also significant fines for 23andMe (£2.31m) and LastPass (£1.2m) for various failings in relation to the security of personal data.
Overall, the ICO issued eight penalty notices for breaches of the UK GDPR in 2025/26 (totalling £32,402,373) and two enforcement notices. For a regulator often described as lacking teeth, this is proof that it can bite where appropriate. This will be an area to watch closely in the coming year to see if the uptick in enforcement action is a sign of things to come under the revamped regulator, or whether it is merely a result of investigations happening to conclude in the same year.

Where formal enforcement action has been taken, a recurring theme continues to be security of personal data. In this regard, the fine issued to Scottish Charity Birthlink (£18,000) should highlight to organisations that a controller's security obligations under the UK GDPR not only apply to digital records - security measures over hard copy personal records are just as important.

Additionally, the Report shows increased enforcement activity in the ICO's key areas of priority, particularly around children's data, fining Reddit and MediaLab.AI for failures relating to age assurance and the lawful processing of children's data.

In relation to the Privacy and Electronic Communications Regulations ('PECR'), the ICO issued ten monetary penalties (totalling £1,445,000) alongside ten enforcement notices. This included a £300,000 fine issued to Home Improvement Marketing for so-called 'robocalls', and a £120,000 fine issued to Allay Claims for sending over 4 million unlawful text messages. Notably, the value of the fines issued continues to be below the maximum threshold of the old regime (i.e. £500,000).

From 5th February 2026, the regulator now has power to impose fines of up to £17.5 million or 4% of global turnover for breaches of PECR. Although the ICO has yet to apply the higher fines, the significant increase in the financial penalties that can now be imposed demonstrates the seriousness with which infringements of PECR are to be treated.

The enforcement trends point to two immediate priorities. First, organisations should continue to review security measures implemented to protect both digital and physical records (with a particular focus on accountability, testing, incident response and remediation). Secondly, organisations should treat the ICO's increased fining powers as a cue to revisit their own PECR compliance with an emphasis on direct marketing and the use of online tracking technologies.

## Children's privacy remains a key focus

No area received greater attention in the Report than children's privacy, leaving little doubt that this will remain one of the regulator's flagship causes.

*No area received greater attention in the Report than children's privacy, leaving little doubt that this will remain one of the regulator's flagship causes*

The Report claims the ICO's engagement with major online platforms has already driven improvements benefiting millions of children, noting the regulator's work continues to focus on social media, video-sharing platforms and online gaming.

Through its Age-Appropriate Design Code, the ICO continues to emphasise that online platforms are responsible for embedding appropriate safeguards to protect children by design. The practical significance of this extends far beyond social media companies. Given the ICO's continued focus in this area, all digital services providers should be proactively assessing whether children are likely to use their services (even if children are not the intended audience) and design appropriate safeguards accordingly. Particular attention should be given to profiling, recommendation systems, behavioural advertising, transparency, and parental consent mechanisms.

The Report highlights the increasing coordination between the ICO and OFCOM in this area, demonstrating how the worlds of online safety and the protection of children's data are becoming increasingly intertwined.

If digital service providers only take away one action point, it should be to assess whether children are likely to use their services. The output of that assessment should be appropriately documented along with any actions that may be required in respect of age assurance, profiling, advertising and transparency. As one of its key priorities, it is increasingly likely that the regulator will expect digital service providers to be able to provide evidence that due consideration has been (and will be) given to children's privacy in respect of their services.

## AI moving from policy to action

The publication of the ICO's AI and biometrics strategy has marked another important shift. Previous reports largely focused on providing guidance and supporting innovation. The Report demonstrates a transition towards active regulatory scrutiny of AI systems and automated decision-making.

The regulator's most notable ongoing investigation in this space relates to the generative AI platform 'Grok'. The ICO is examining not only whether Grok's processing of personal data is lawful, fair, and transparent, but also whether the AI model has incorporated adequate safeguards against harmful and manipulative outputs using personal data.

Additionally, as part of its AI and biometrics strategy, the Report refers to the ICO's audit of central government and the recruitment industry looking at the use of automated decision-making. These are some examples of the proactive regulatory intervention undertaken within the realms of AI and automated decision-making, which is expected to increase over the coming year as regulators start to build a sectoral picture of how these technologies are deployed in practice.

What's clear is that as the ICO (and other regulators) continue to take greater interest in the deployment of AI capability, it will be essential for organisations to

establish comprehensive AI governance frameworks rather than relying on a data protection impact assessment. Transparency obligations, fairness and bias testing, appropriate supervision, and ongoing monitoring will all have a role to play.

Effective AI governance does not have to be complicated. At a basic level, it starts with clear ownership and oversight, careful handling of personal and sensitive data, recording how AI is being used and the decisions that are made around it. The organisations that manage it well are likely to be those that build on existing privacy and governance practices rather than creating a separate accountability regime in isolation.

In the meantime, we await further guidance from the regulator on the use of AI through its statutory AI code of practice. This continues to be progressed into 2026/27 and will no doubt provide prime bedtime reading for DPOs and privacy professionals once published.

## Unprecedented complaints pressure

One of the most notable trends in this year's report is the sheer volume of public engagement. The ICO received 76,743 data protection complaints (almost double from the previous year) and 10,713 Freedom of Information complaints. Despite the introduction of a new complaints handling process designed to deliver faster and more impactful outcomes, the marked increase in complaint volumes has significantly hampered the ICO's ability to meet its own key performance indicators. By way of example, the ICO was only able to assess and respond to 27.4% of complaints within 90 days and 69.5% of complaints within six months (against 30% and 98.4% in the prior year).

The regulator's take on the pressures exerted by the increased volume of complaints is that it shows a positive shift in greater public awareness of information rights (and confidence in using them). For organisations facing a regulatory complaint, knowledge that complaints are unlikely to be assessed for a lengthy period of time provides a greater window of opportunity to further consider their compliance posture and take mitigating steps where necessary.

In any event, organisations will now be expected to shoulder some of this burden in the coming year due to the new complaints handling regime introduced by the DUAA (inserting new section 164A into the Data Protection Act 2018). The ICO will certainly hope that organisations can triage and address complaints themselves minimising the need for further escalation to the regulator. It remains to be seen whether the new complaints regime will have any impact on the volume of complaints made to the regulator each year.

The new complaints-handling regime took effect on 19th June 2026. Organisations should now check that they have internal complaints procedures to ensure that complaints can be appropriately acknowledged, assessed and addressed in compliance with the new regime without undue delay. The ICO will expect organisations to attempt to resolve complaints effectively before regulatory escalation becomes necessary.

## Public sector accountability and organisational assurance

The Report also provides an update on the ICO's approach to regulating the public sector and improving organisational capability.

In January 2026, in the wake of a number of serious data protection breaches within government, the ICO and central government signed a Memorandum of Understanding establishing expectations around coordinated accountability, consistent standards, training, and annual assurance reporting. The Memorandum of Understanding emphasises institutional accountability rather than individual compliance failures.

The Memorandum of Understanding reads like the regulator's articulation of what good accountability looks like (particularly in the context of large federated or group organisations). It is expected that the regulator will increasingly expect organisations to demonstrate compliance being embedded within governance systems rather than dependent on individual expertise or isolated compliance advice.

For organisations trying to understand what the regulator is looking for, the Memorandum of Understanding is a good place to start. Accountability is increasingly being framed as an organisational capability, rather than a matter

of individual responsibility or just having the right policies in place. Organisations must be able to demonstrate that they not only understand their data protection obligations and have appropriate policies and procedures in place, but that they have appropriate governance and assurance frameworks needed to deliver them consistently in practice.

## Where is the scrutiny heading?

The Report is less of a retrospective account of regulatory activity and more a statement of regulatory intent for a fresh start for the regulator. It points to a regulator that is increasingly focused on governance, technology, and organisational behaviour with AI, children's privacy and cyber resilience forming just some of its key priorities.

Organisations should take this opportunity to review and strengthen their internal frameworks, paying particular attention to the regulator's priority areas. It is clear that, going forward, the regulator will expect to see genuine, organisation-wide commitment to data protection, not just compliance for its own sake. The best prepared organisations will be those that continue to prioritise appropriate governance frameworks for the implementation and use of new technology and incorporating privacy by design throughout.

By continuing to take proactive steps now, organisations will be better equipped to meet future regulatory scrutiny and garner trust from both the regulator and the public.

**Daniel Bishop**
daniel.bishop@stephensonharwood.com

**Alison Llewellyn**
alison.llewellyn@stephensonharwood.com

**Katie Hewson**
katie.hewson@stephensonharwood.com

**Sarah O'Brien**
sarah.obrien@stephensonharwood.com

Stephenson Harwood