The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

Dame Chi Onwurah MP
Chair
Science, Innovation and Technology Committee
House of Commons
London
SW1A 0AA

Our reference: ICO/O/JE/L/SEL/0822
By email to: commonssitc@parliament.uk

04 November 2025

Dear Chair,

Thank you for inviting me to give evidence to your committee. I agreed to follow up on a number of issues which I set out below.

The ICO's handling of sensitive and classified information

The committee asked for more details about how the ICO handles sensitive information. We deal with tens of thousands of different data protection issues a year through our complaints, investigations, audits, breach reports and engagement. The vast majority of the information we work with can be handled in our normal case management systems, with restricted access where appropriate and by staff with appropriate security clearance.

In rare cases we work with information that is highly sensitive which requires handling outside of our normal systems. My office already has staff with the appropriate security clearance to handle sensitive information, and I am taking steps to increase that number. In addition, we also have physical and digital provisions to handle sensitive information. We can store this information, record and carry out our work, and communicate with relevant stakeholders using secure channels to discuss classified information. I have not provided more specific detail here for security reasons.

However, in an even more limited set of cases there are additional restrictions on how we can handle sensitive information. These cases make up a tiny fraction of our total work. The 2022 MoD data breach was one of these cases, but had additional complexity due to the handling restrictions imposed on us by the MoD because of the very high classification of the information. These restrictions limited our ability to take contemporaneous notes or keep details about our decision making at that time.[1]

A member of the committee asked me about the seniority of the MoD staff we engaged with throughout the process. I can confirm what I said during the committee session, which is that my staff dealt mainly with the data protection officer and his team as they were best placed to engage on the operational detail required. As part of this engagement, my staff also met with other officials including parts of the MoD's legal team where relevant. This engagement across relevant MoD staff included officials at senior civil service level.

How the ICO works to raise standards around the use of information in the public sector

The committee expressed an interest in the role of the ICO in monitoring the government's use of third party outsource partners, particularly those offered to non-UK companies.

All organisations including government, in their capacity as data controllers, are responsible for ensuring personal information is used in accordance with the law. A vital part of this is securing the appropriate agreements with third parties who carry out work on their behalf, often as data processors. Any public sector organisation entering into such an agreement must only use third parties who provide sufficient guarantees that the use of personal information complies with the law. This includes having the appropriate security measures in place to protect personal

[1] record-of-mod-data-breach.pdf

information and clear agreement around any international transfers of information.

We have a number of ways in which we work with the public sector to improve data protection practices and ensure compliance with the law. We publish detailed guidance[2] and templates[3] to help organisations navigate the law and manage risk. This provides organisations with the means to put in place the measures necessary to protect people's personal information.

We provide direct, practical input through policy engagement with central government and the wider public sector, including on the federated data platform referenced in the session and through events like our annual conference, held this year on 14 October where we delivered information to nearly 7,000 data protection practitioners. We are also working to drive up standards across the public sector and to ensure data protection is treated with the seriousness it deserves at senior level[4]. This work is vital not only to guard against the types of risk raised by the committee, but in order for the government to achieve its ambitions to digitally transform public services.

We use our range of supervisory powers where we have reason to believe personal information is not being used in accordance with the law. We deal with tens of thousands of complaints each year, receive and respond to thousands of personal data breach reports, and conduct investigations into cases where we can have the greatest impact in preventing future harms.

Since April 2023, our audit teams have worked with 80 public sector organisations, making recommendations and then following up on these to check progress. This resulted in 1981 recommendations being made across the public sector, with over 95% being accepted in full or in part,

---

[2] Controllers and processors | ICO
[3] Contracts | ICO
[4] Update on our work to raise data protection standards in the public sector | ICO

and over 98% of these actioned or in progress at the follow-up stage. Since the introduction of our public sector approach, we have used significantly more reprimands to tackle issues in the public sector such as subject access request backlogs and security failings. During the first two years of the approach we issued 77 reprimands, a 54% increase on the previous two years, with 80% of these targeted at the public sector.[5]

We've taken action for serious security failings by organisations that work across the public sector. This year we issued a fine of £3.07 million to Advanced Computer Software Group which acts as a data processor and provides IT services for a number of public sector organisations including the NHS[6]. The fine related to a ransomware attack in 2022 which put the personal information of over 70,000 people at risk and was caused in part by the lack of multi-factor authentication, a key technical security measure.

Earlier this month, we fined Capita, one of the biggest outsourced providers of public sector services, £14 million in relation to a 2023 breach which led to 6.6 million people's information being stolen[7]. We found that Capita had failed to ensure it had appropriate technical and organisational measures to protection information, including failures to respond appropriately to security alerts, failure to prevent privilege escalation and inadequate penetration testing and risk assessment.

Our investigations into the use of children's personal information

The committee asked about the progress we had made on a number of investigations into children's privacy.

To expand on my evidence on our 2023 fine for TikTok's use of children's data without parental consent, the Upper Tribunal has now granted TikTok permission to appeal the First-tier Tribunal's decision that the ICO

[5] https://ico.org.uk/media2/migrated/4032016/psa-post-implementation-review-report.pdf
[6] Advanced Computer Software Group Limited | ICO
[7] Capita fined £14m for data breach affecting over 6m people | ICO

can impose the fine against them, after the FTT previously refused permission. A date for the Upper Tribunal hearing has been set for May 2026, more than three years after our penalty decision was issued. Even if this preliminary issue is ultimately determined in our favour, there may be an onward appeal to the Court of Appeal and, ultimately, the matter will still need to go back to the FTT for it to hear the appeal on the substantive issues. The delays in this case are not unusual, but it is a good example of the length of time it takes for our decisions to work through the appeals process with appeals starting in the First-tier Tribunal.

I also explained to the committee that we commenced a separate investigation in March 2025 into how TikTok uses children's personal data to make recommendations to them. TikTok appealed the Information Notice we issued as part of this investigation. A date for this appeal hearing has not yet been set as the proceedings have been stayed by the FTT pending determination by the Upper Tribunal of TikTok's appeal against the MPN dated 4 April 2023. This means that our investigation into this important matter is delayed by matters outside of our control.

Deepfakes and Doxxing

The committee raised questions about the practice of outing people's personal information known as 'doxxing', and about deepfakes.

While I acknowledge that these practices can be very distressing and harmful to the victims, there are significant limitations to our remit which preclude us from taking action in many cases.

The law provides that individuals are not bound by data protection principles when personal information is used for 'personal or household' purposes[8]. An activity such as people creating content for their own use

[8] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/

or to be shared with a limited audience would therefore often not be subject to our jurisdiction.

Such activities are more likely to engage online safety legislation and the criminal law. We work closely with Ofcom which plays a significant role in holding platforms to account for managing the content that people post to their platforms, focusing on illegal content and content that is harmful to children. The Online Safety Act, which is administered and enforced by Ofcom requires platforms to take a number of measures, including responding to complaints and taking steps to prevent and remove illegal content and content that is harmful to children.

Maliciously targeting someone online can also be a criminal offence, under harassment or malicious communications laws. Creating, requesting the creation of or sharing intimate images of someone without their consent will become an offence under the Sexual Offences Act 2003 once the provisions of the Data Use and Access Act are commenced.

I hope the above is helpful to the committee. I look forward to updating you on the important work we are doing with government, including publishing a joint commitment by the end of this year, to improve standards across government. This work is vital to reduce the risk of a similar breach happening again. Please do feel free to get in touch if you have any questions.

Yours sincerely,

John Edwards
UK Information Commissioner