# Memorandum of Understanding (MOU) between the Information Commissioner's Office and His Majesty's Government

## Summary

This MOU builds on and formalises the Information Commissioner's Office (ICO) and His Majesty's Government's (HMG's) approach to working effectively in line with our respective roles to protect people's information.[1] It sets out an enduring framework and approach to co-operation and collaboration and is not intended to be exhaustive.

## MOU parties

The parties to this MOU are HMG and the ICO. The Department for Science, Innovation and Technology (DSIT) and the Cabinet Office act on behalf of HMG in this MOU and are responsible for leading work to implement its commitments.

Nothing in this MOU creates legal obligations that can be enforced by any party. It reflects the mutual intentions and understandings of the parties.

## The ICO's role as an independent regulator

Both the ICO and HMG recognise the independence of the ICO and its role of regulating to protect people and enable responsible data use and innovation. It does this through providing expert advice which relies on government being provided appropriate and timely information. Nothing in this MOU overrides the government's statutory obligations or interferes with the ICO's role to hold government to account as an independent regulator. Nor does it prevent any appropriate regulatory intervention with government departments to ensure compliance.

## Purpose and shared vision

The parties have a shared interest in public authorities providing services that are personalised, accessible, convenient and efficient. The ICO supports the government's ambition to use new technologies to transform public services, create a modern digital government and drive economic growth.

Both parties believe that this transformation relies on the public having trust and confidence that their data is being used safely, for the public good and within the law.

Both parties are therefore committed to continuous improvement in how we work together.

[1] Statement on the public sector approach | ICO December 2024

This MOU sets out a shared understanding of working towards better government data security and use.

## Shared principles and joint commitments

Ministers and senior officials are committed to the ICO's public sector approach which prioritises engagement and accountability at a senior level to drive high standards of data protection compliance, preventing harms before they occur and learning lessons to improve practice when things go wrong.

Both parties agree to:

- Work together to ensure the public can see real benefits in sharing their data and trust that it will be protected.
- Work collaboratively and transparently, taking a 'no surprises approach' – this will require a free flow of information about our work and processes.
- Ensure that there are regular meetings between the signatories of this MOU to review the progress and relevance of the MOU every 12 months.
- Jointly provide an update on our work together on a regular basis.

## Ensuring compliance and creating a data safety culture

**The government will:**

- Publish an annual assurance statement on how people's data is being kept safe and how new and proposed technologies and processes have been designed with trust and privacy in mind.
- Commit to prioritising public trust and confidence in the government's handling of personal data by investing the appropriate resources and time needed to continue to create a culture of high standards and compliance. Ministers and senior officials will take an active lead within and between their departments to improve the culture of safeguarding people's data.
- Establish a cross-government culture of continuous learning around improving information security. This includes gathering intelligence and learning lessons from personal data breaches and 'near misses'

and implementing actions that would prevent a future similar breach.

- Set a clear process for responding to a personal data breach and ensure that all civil servants follow this process and that it is updated as required.

- Seek the ICO's expert advice when it has identified that the use of personal data in the delivery of a policy or a system carries a significant risk. This will require government to provide transparent and timely information to the ICO. This does not replace the government applying its own appropriate internal scrutiny and advice in line with their statutory obligations.
- Ensure that at all times there is an accountable and named individual responsible (currently the Government Chief Data Officer) for managing cross-government data protection risk and compliance. Resource a central team that will set consistent standards, respond swiftly to risks identified through departmental reporting and insights, advance privacy technology across government and work with department data protection officers.
- Raise awareness of civil servants on how to share data safely, protect personal data, and improve their information management, through guidance and training.

- Inform civil servants of the real-world consequences of inadvertent personal data breaches, by developing and delivering ongoing and engaging communication campaigns.

- Track key indicators that monitor civil service maturity and awareness of information management.

**The ICO will:**

- Champion the safe use of personal data for the public good.
- Provide regulatory certainty by producing timely and relevant products including guidance, codes of practice, advice notes, opinions and audits that support government and the public sector to use people's data safely.
- Be transparent with the public when holding an organisation to account for a breach. Encourage government, and other public sector organisations, to learn lessons from the ICO's work and use these as an opportunity to review and improve their own practices.

- Use its expertise and resources to enable a government communication campaign to make staff aware of real-world consequences of personal data breaches and provide expert advice with training and the development, use and updating of a government 'model action plan' following a breach.
- Use its intelligence, including from breach reports and contact with the ICO advice services, to identify trends and potential risks and share their insights and trends with government to take action.
- Provide independent and expert advice in response to government raising a substantial risk. This does not replace government's own internal scrutiny, including where necessary seeking other external advice. The ICO will also promote good practice within government when found.
- Additionally, the ICO will recognise that senior responsible officers in DSIT and Cabinet Office are responsible for driving collaboration between departments and the ICO will work with both officers to support that.

## Early engagement in design of projects and new uses of people's data

The ICO and HMG will work together on the government's ambition for new uses of public sector data to transform people's lives by improving the delivery of public services while boosting economic growth.

**The government will:**

- Be responsible for ensuring that projects involving the innovative use of personal data or new technologies embed a privacy and trust by design approach
- Ensure new projects are brought to government department boards and to the appropriate senior level cross-government governance group, such as the Technology Risk Group, to ensure oversight of any risks and to provide constructive challenge to the accountable officers responsible for projects brought to the boards.
- Actively seek, at an early stage, the ICO's expertise, constructive feedback and advice with innovative projects that use personal data. The government will need to be transparent and provide all relevant information to the ICO. The government remains ultimately responsible for compliance.

**The ICO will:**

- Continue to provide independent expertise, supportive challenge and advice to government as it develops new use cases of personal data and technology.
- Use its range of innovative services, including our regulatory sandbox and innovation hub, to support government and other public sector organisations.
- Use insights gained from working with government on new uses of data to ensure its guidance and other products are updated and relevant

## Reporting and accountability

To ensure public confidence and trust in the use of their personal data the ICO and HMG believe we should be transparent about our work together.

**The government will:**

- Publish an annual assurance statement on GOV.UK on how people's data is being kept safe and how new and proposed technologies and processes have been designed with trust and privacy in mind.

- Provide effective oversight through an accountable governance model reportable to the Transformation Board (formerly Operations Board). This will include department boards and risk and audit boards regularly monitoring department-wide data protection risks and tracking the progress of measures set out by the Government Chief Data Officer. This process will also act to prevent, as well as resolve, issues and ensure significant data and information security risks are visible at the highest levels of government through the oversight of the Technology Risk Group.

- Carry out regular assurance exercises within departments, including using the information security checklist, that provides visible accountability to department boards and risk and audit boards as well as senior cross-government boards (for example the Government Security Board and the Transformation Board).
- Keep in regular communication with the ICO to maintain a level of assurance with the regulator. Ensuring that government meets the standards the ICO expects of us. Government will do this by

regularly sharing any key findings of assurance exercises it carries out and progress on remediation following a major data breach.

- Invite the Information Commissioner to attend the Transformation Board (formerly Operations Board) and the Government Security Board on a six-monthly basis.

**The ICO will:**

- Work with government to use insights from assurance exercises to inform the development of guidance and other resources.

- Attend the Transformation Board and Government Security Board on a six-monthly basis to receive assurance and provide independent expert advice.

## Declaration and signatures

We the undersigned agree that this MOU formalises the ICO and HMG's approach to protecting people's information. It sets out an enduring framework and approach to co-operation and collaboration but is not intended to be exhaustive.

**The Rt Hon Ian Murray MP**

Minister for Digital Government and Data

Minister of State at the Department for Science, Innovation & Technology

**Dan Jarvis MBE MP**
Security Minister
Minister of State at the Cabinet Office

**John Edwards**

UK Information Commissioner

***8th January 2026***