Cabinet Office

Department for Science, Innovation & Technology

Dame Chi Onwurah MP
Chair, Science, Innovation and Technology Committee
House of Commons SW1A OAA

20 October 2025

Dear Dame Chi,

The Chief Secretary to the Prime Minister and the Secretary of State for Science, Innovation and Technology have asked us to follow up on correspondence from 28th August, outlining further measures we intend to take to raise information security standards, ahead of the forthcoming Select Committee session on this subject.

Central to these measures will be a step-change in how data protection is coordinated in government. Government Digital Service within the Department for Science, Innovation and Technology will take on responsibility for coordinating cross-government data protection risks and compliance. The Government Chief Data Officer (GCDO) will be the accountable individual responsible for managing cross-government data protection risks and compliance. We will establish a new, dedicated team reporting directly to the GCDO who will set consistent standards, respond swiftly to risks and advance privacy technology across government.

Alongside this, Government is drawing up a joint commitment with the ICO to work together to raise standards. The commitment will create a proactive mechanism for us to seek the ICO's expertise and facilitate constructive feedback. Together, these measures will be a significant step towards building a more effective and accountable governance model for the protection of citizen data within government.

Significant data and information security risks must be visible at the highest levels of government. A cross-government Technology Risk Group will be established and chaired by DSIT to drive accountability for technology risk, unifying all major technology risks under one clear and accountable governance structure. The Technology Risk Group will report to the Operations Board and update the Digital Inter-Ministerial Group. The Government Security Board, chaired by the Cabinet Office, will track overall progress against the measures set out below. The ICO will be invited to Operations Board and Government Security Board meetings to support ongoing collaboration and continuous improvement

We are working on additional measures across four key domains as follows:

Government policy and processes

We will ensure that the right senior officials across government are responsible for managing

down risks of further data breaches, and that we get the response right if they do occur. To that end, the Cabinet Office will deliver the following measures:

1. Cat Little, the Cabinet Office Permanent Secretary and Emran Mian, the Department for Science, Innovation and Technology Permanent Secretary will run an assurance exercise for all central departments and arms-length bodies in October 2025, setting out measures and processes departments must have in place. This will help build out a risk profile across government to inform priority areas for the Government Chief Data Officer and their new team.

2. To ensure that existing controls adequately address the risk of recurrence, Cat Little will also write to all risk and audit committees to review their department's risk appetite towards threat to life data breaches.

3. To go one step further, the Government Chief Security Officer will lead an exercise with all Security Advisors and Heads of Knowledge and Information Management to review departmental information asset registers to understand if any high-risk personal data sets can no longer be tolerated at the OFFICIAL classification tier.

4. We need to have robust plans in place for when data breaches do happen. GSG will work with the ICO and the Government Chief Data Officer in GDS to develop a ‘model action plan’ for Security Advisors and Data Protection Officers in the event of a breach.

GDS will deliver the following measure:

5. To improve how large, aggregated personal data sets are managed, GDS will ensure that all departments are following the principles for securing personal data in government services (published in June 2025) when running systems or services which process or share personal data. In particular, we will apply these principles when building new services such as Digital ID.

Technology

Technological interventions can play an important role in mitigating the risk of data breaches. To that end, DSIT will deliver the following measures:

6. To drive full value from government’s critical IT partners, we’re strengthening strategic relationship management - starting with Microsoft, the backbone of government’s digital workplace. DSIT’s Digital Commercial Centre of Excellence (DCCoE) will coordinate across departmental commercial functions to hold Microsoft to account for reducing the risk of accidental data breaches by maximising value from its tools. Priorities include fixing critical information security gaps, ensuring consistent use of data loss prevention features and embedding best practice. DCCoE will work with GSG and NCSC to provide the guidance departments need to get more assurance and benefit around protecting

citizen data from this partnership.

7. Departments need better tools to protect sensitive data in everyday digital workflows. Data Loss Prevention (DLP) can stop accidental sharing, but inconsistent adoption has limited its impact. GDS is working with Microsoft to test a simpler, layered approach and set a clear baseline for DLP use. The Government Security Centre for Cyber will also continue to provide their Optimising Microsoft Security Solutions support service to departments implementing the Microsoft Purview Information Protection guidance.

Culture

Fundamentally good information security also needs to become habitual for all civil servants. We will do this by:

8. GSG will commission the Security Education and Awareness Centre to issue a new communications campaign by Q1 2026, which makes staff aware of the real-world consequences of inadvertent data breaches. GSG will also bid to the Cabinet Secretary to make Information Security the focus of the 2026 One Big Thing campaign.

9. Accidental data breaches often result from general poor information handling. To help fix this, GDS will support government information management professionals to ensure they have the authority and skills to help staff protect sensitive data. GDS will also roll out new information management training for all civil servants.

Relationship with the ICO

Underpinning all of this, we intend to strengthen our relationship with the ICO to ensure our work reflects the standards the regulator expects of us.

10. Government will draw up a joint commitment with the ICO to work together to raise standards by the end of 2025. The commitment will create a proactive mechanism for us to seek the ICO's expertise and facilitate constructive dialogue.

11. To reinforce this commitment, the ICO will periodically be invited to the Operations Board and Government Security Board to support collaboration and continuous improvement.

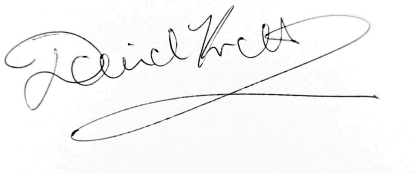
As the Senior Responsible Officers for the respective policies in each department, the Director for Security Policy and Strategy in Cabinet Office and the Government Technology Officer in DSIT will be responsible for driving collaboration between departments.

We have copied this letter to: the Information Commissioner; the Chair of the Defence Committee; the Chair of the Public Administration and Constitutional Affairs Committee (PACAC); and the Chair of the Intelligence and Security Committee.

Yours Sincerely,

Vincent Devine,

Government Chief Security Officer



David Knott,
Government Chief Technology Officer