Microsoft 365 outage
Oral Statement, Monday 16 November 2026

Embargoed until the Rt Hon Ian Murray MP, Minister for Creative Industries, Media and Online Safety has sat down after his initial speech

**** Check Against Delivery ****

With permission, Mr Speaker [or Madam Deputy Speaker], I will now make a Statement on the Microsoft 365 outage.

Mr Speaker, on Thursday 12 and Friday 13 November 2026 we saw an outage affecting Microsoft IT systems which caused impacts around the world. Users of Microsoft products were unable to send and receive emails, nor use a range of other Microsoft products and services.

This was a serious incident which caused disruption for a lot of people and businesses.

Microsoft initially explained that the incident was caused by "elevated load" on its infrastructure, and later provided further details on the three main issues which led to the outage. The company said there is no indication the incident was caused by malicious activity.

In the UK, this incident affected individuals, businesses and the public sector. There were impacts on the health sector and other public services. But key services such as 999 remained operational.

There were no major critical services impacts and public sector resilience plans are in place.

This incident could have been more serious if it had lasted longer. It reinforces the importance of promoting and improving our digital resilience, something the government is already taking significant action on.

There was some organisational disruption in local government, where many organisations are reliant on Microsoft products. Multiple Local Resilience Forums were stood up to provide support and coordination amongst local services.

This incident also caused disruption across businesses of all sizes. Staff were unable to carry out their normal work duties. Firms were unable to complete their usual transactions.

Members and staff in this place were also affected.

We recognise the disruption this has caused to people and organisations, and we are still working to understand the full impact. However, I would like to highlight how critical and important services remained available and in operation across the country.

Accident and emergency departments remained open. Transport services were unaffected by this outage.

There were no known issues with UK mobile, broadband, or landline connectivity. Major telecoms providers confirmed their services were working as normal.

We currently have no evidence of wider impacts to UK data centre infrastructure or other cloud operators, and no such impacts have been reported to us by industry at this stage.

There were no reported impacts to water or wastewater treatment processes.

Businesses, including shops and services, remained open across the UK.

By Friday afternoon, Microsoft systems were coming back online and services were returning to normal.

Mr Speaker, the government takes this issue very seriously.

Public sector organisations and government departments have plans in place for these exact situations, to mitigate potential impacts and ensure the continuation of operations.

The Department for Digital, Culture, Media and Sport is the lead government department for national digital resilience issues.

As soon as we became aware of the problem on Thursday evening we made contact with Microsoft to start discussions on the issue, assess the impact and request details of how the problem was being resolved. My colleague, the Minister for Cyber Security [Baroness Liz Lloyd], spoke to the CEO of Microsoft UK on Friday.

My officials in DCMS led the co-ordination of the response across government departments, in collaboration with the Cabinet Office.

We expect Microsoft to share their lessons learned from this incident. We will be engaging further on how they will prevent such incidents happening in the future and plan for swifter remediation of incidents to limit service disruption.

Digital services, like the cloud computing services Microsoft provide, are already regulated under the UK's Network and Information Systems Regulations 2018.

This requires providers to manage security and resilience risks, prevent and minimise the impact of incidents, and report significant incidents, including non-malicious system failures.

Our Cyber Security and Resilience Bill strengthens that framework further. It strengthens and clarifies the duties applying to cloud providers, brings data centres and managed service providers into scope, and enables security and resilience requirements to be updated as risks evolve.

Mr Speaker, in the UK we have adopted and benefited from new technology faster than many other nations. This has powered our economy and enabled growth and innovation. However, in an environment where we are so dependent on technology, we do need to make sure our systems are resilient and that we have plans in place for when there is disruption. This will ensure that where there are problems, we can recover faster.

This is true for both government and industry.

In parallel, we are also working to diversify government's supply arrangements, including backing small and medium sized British suppliers. By using government's collective buying power we can encourage a more competitive and resilient technology market - for example, through the National Cloud Infrastructure Programme, which will improve resilience by diversifying supply options and enabling government to contract for cloud services at a whole-of-system level.

Mr Speaker, the first duty of any government is the protection of its citizens. This is why we have been taking significant action to improve resilience across the nation.

The Government Cyber Action Plan, published in January this year, sets out how we will improve cyber security and digital resilience across government and the public sector.

I've already mentioned our Cyber Security and Resilience Bill which is currently in Parliament. The Bill will boost UK cyber defences and improve the resilience of our essential and digital services.

In the recent budget we committed £500 million pounds to build the secure foundations for an AI-enabled economy, including measures to strengthen the public sector technology estate.

A cross-Whitehall Technology Risk group for UK Government is now established. It is actively reviewing and overseeing the response to our major strategic risks.

We have recently established a Chief IT Operations function for UK Government, and it has been key to our work on the recent incident. Its critical role will be to systematically review post-incident reports, service outages and performance, and to work with IT Operational, Commercial and Financial Leads to develop future interventions that strengthen public sector resilience.

The future Technology Plan will set out Operational Standards and Practices for Firmer Foundations across UK Government. This will be alongside accelerating an intensive baselining of the Public Sector technology stack, technical health and dependencies.

We take these actions as any responsible government would do – to protect our citizens, our businesses and our economy.

Mr Speaker, this outage, like the Crowdstrike incident in 2024, shows how dependent our economy is on interconnected IT systems, and why resilience planning matters. We have also seen in the US how outdated technology can have an impact on services the public rely on.

My department will now be working with partners across government and industry to fully understand the impacts of this incident and gather any further lessons learned. We will use this work to strengthen our resilience.

In that spirit, I commend this Statement to the House.