Response to the November 2025 *Economic and fiscal outlook* publication error

Background and summary of response

1 On 26 November 2025, the day of the 2025 Budget, premature access was secured to the OBR's *Economic and fiscal outlook* (*EFO*) by external users, shortly before the Chancellor's speech. The non-executive members of the OBR's Oversight Board led a rapid investigation into that error, supported by expert technical advisor Professor Ciaran Martin and OBR and Treasury staff, and the investigation report was published on 1 December.[1]

2 This investigation discovered a technical misconfiguration on the OBR's website that meant protections were not properly in place to stop those seeking premature access to the document. It made recommendations to the OBR and others – which the OBR accepted in full – on the steps that should be taken to further examine this error, address it, and rebuild trust. This short report provides a summary of the progress that has been made against these recommendations to date. It also provides details of how the OBR has approached online publishing of *EFO*s and other sensitive material, and broader information security, since the November incident. This report is being published alongside the OBR's 2025-26 annual report and accounts to support the Budget Responsibility Committee's and non-executive members' account of the error and the response to it in the annual report.

3 A summary of the recommendations of the initial investigation, and in each case a brief account of work that has been undertaken by the OBR and others in the months since, is as follows:

- An **external deeper investigation into recent *EFO* publications**. This was conducted by the National Cyber Security Centre (NCSC), and published on 9 February 2026.[2] This fuller investigation confirmed many of the findings of the initial investigation, including the fact that the incident occurred because of a misconfiguration of the way in which the WordPress platform was implemented. The NCSC had access to more logging data than the initial investigation and as such found that the scale of early access to the November 2025 *EFO* was much greater than initially reported, although the vast majority of these accesses occurred after the *EFO* content had started being broadcast by media outlets. The key recommendation of the NCSC investigation was that future market-sensitive OBR publications are published on GOV.UK.

[1] OBR, *Report of investigation into the November 2025 Economic and fiscal outlook publication error*, December 2025.
[2] NCSC, *Early access to OBR Economic and Fiscal Outlook: NCSC analysis and technical recommendations*, February 2026.

- A working group to **establish suitable short- and medium-term arrangements for the OBR's online publishing and overall web presence**. This working group was formed in December 2025 – made up of staff at the OBR, the Treasury, the NCSC and the Government Digital Service (GDS) – and has met regularly since. It has advised the OBR's leadership on and approved various aspects of the response, including ongoing use of the OBR's current website for non-sensitive material, the approach to publishing the March 2026 *EFO*, and development of the OBR's longer-term web publishing solution. These are all detailed further in the sections below.

- Regular **broader external reviews of the OBR IT and security arrangements**. The Treasury agreed to provide the initial iteration of this as part of its *Budget Information Security Review*, which was published on 9 February alongside the NCSC investigation.[3] This provided a summary of the OBR's IT and security practices during forecasts and made recommendations for changes, including new security classifications to further protect both the most-sensitive policy information and the wider body of forecast information that regularly flows between the OBR, the Treasury and other departments. It also committed to the OBR, Treasury and the Bank of England working together to produce shared protocols for any future early release of market-sensitive information, which these organisations are now developing.

- Proactive **cooperation with the Financial Conduct Authority (FCA) and any other investigations**. The OBR has been cooperating proactively with the FCA since the incident. OBR staff have also completed FCA training on identifying and handling inside information, and we are exploring other relevant training options.

- A **review of arrangements for handling sensitive material by other agencies of government**. This is beyond the scope of the OBR's own activities, but the Government Internal Audit Agency is undertaking a review of cross-government publishing on behalf of the Cabinet Office and the Department for Science, Innovation and Technology. Its aim is to validate and strengthen the effectiveness and consistency of publication processes on GOV.UK and on non-GOV.UK websites, particularly with respect to sensitive information.

4 The remaining sections of this report provide further details on aspects of the response mentioned above.

Publishing the March 2026 *EFO*

5 Following the NCSC recommendation that all future OBR market-sensitive publications should be published on GOV.UK, the OBR worked rapidly with Treasury publishing staff to develop a plan for publishing the March 2026 *EFO* in this way. The plan was agreed by the working group on the OBR's future web publishing approach, and involved the Treasury initially publishing the *EFO* at the market-sensitive moment on GOV.UK, as an independent report on its own site, with the OBR subsequently linking to this document and adding

[3] HM Treasury, *Budget Information Security Review*, February 2026.

supporting documents on its own website. These protocols were designed to provide the best balance between security and timeliness.

6 This approach was implemented successfully on 3 March, with OBR staff preparing the relevant webpage content in draft in the Whitehall publisher platform, which was then submitted shortly before the intended publication time to be verified by Treasury staff, and pushed live to publication by Treasury staff just after the Chancellor's statement had concluded at 12:57. Once the *EFO* was visible on GOV.UK, at 13:02, OBR staff updated the OBR website to link to the document from the OBR homepage, and began updating the OBR's website with the supporting documents and supplementary material. This process was complete at 13:43.

7 We judge that this approach was successful because: the *EFO* document was protected throughout the process and not accessed early; the *EFO* was released with only a very short delay after the Chancellor's statement concluded, and the OBR website was fully populated with all the expected content shortly after that; and we received no complaints from stakeholders regarding difficulties accessing the *EFO* or supporting documents.

8 In evaluating this approach, we have reviewed the website logs for obr.uk for any activity indicating attempts to access the March 2026 *EFO* prior to its intended publication time. The logs show there were 543 unsuccessful attempts between midnight the day prior to publication and 12:57 on the day, when the Chancellor's statement finished. For most of these requests there was a clear pattern, with requests being made exactly four minutes apart, indicating a script or similar prepared by one user. All these requests returned a '404 response' because no document was ever uploaded to the server.

Overall approach to the OBR website and web publishing

9 Following the November incident, the OBR implemented improvements to and developed new protocols for uploading non-sensitive material to its current obr.uk website, which included no material being uploaded to servers even in draft prior to the intended publication time. These protocols were approved by Treasury IT security experts. They have allowed the OBR to continue routine business such as publishing news posts, letters, its monthly commentary on the public sector finances, and supplementary *EFO* material after the *EFO* had been initially published on GOV.UK.

10 In parallel, the working group began discussing the requirements under consideration for the OBR's future web presence. The group agreed to requirements that covered areas such as security, maintenance, resource considerations, and the real and perceived independence of the OBR. The group also agreed that the OBR should consider options ranging from fully moving the OBR's web presence onto the GOV.UK infrastructure – perhaps with the ability to build stand-alone web-applications and static pages for specific outputs that are not supported on GOV.UK – to maintaining the OBR's current website as its main online home but using the GOV.UK infrastructure to publish market-sensitive information in the first instance. The working group advised that the OBR should undertake

work to review the feasibility, strengths, weaknesses, security, and resource requirements of each option, as well as engaging with key users on their needs and preferences. This work is now underway.

11 In the interim, drawing on the advice of the working group, the OBR leadership agreed to maintain obr.uk as the OBR's main website and publish statutory reports and market-sensitive information on its own GOV.UK webpage in the first instance, mimicking the approach taken for the March 2026 *EFO*. This interim approach serves as an opportunity to test the merits of some of the longer-term options for the OBR's web presence while reviewing the security of the OBR's existing website. The OBR is working closely with Treasury IT experts on this security-related work, which we plan to include penetration testing, external cyber reviews, targeted self-assessment and audit.

Broader information security

12 The OBR reviewed and strengthened its broader approach to information security during the March 2026 forecast. Steps included: more frequently providing staff with detailed forecast security guidance; increasing the use of restricted links to the internal file storage system to share forecast material; engaging with senior Treasury officials on practices for managing pre-release copies of *EFO* chapters shared with the Treasury prior to publication; and temporarily suspending the practice of publishing aspects of the forecast timetable in advance.

13 These steps went with the grain of the recommendations of the concurrent *Budget Information Security Review*, which recommended further security enhancements that will be implemented by the OBR and other forecasting departments prior to the next forecast.

Conclusion

14 The leadership of the OBR is confident that we either have addressed all of the recommendations of the initial investigation into the November 2025 *EFO* publication error and the subsequent investigations and reviews. We will continue to work with the Treasury and with IT and security experts across government to ensure our approach to web publishing, IT security and broader governance and risk management in these areas meets the standards expected of us. And we would like to again acknowledge the seriousness of the publication error on 26 November 2025 and apologise for the disruption it caused to the Government and Parliament.

15 We welcome feedback on any aspects of our response. This can be sent to feedback@obr.uk.