



HM Treasury

Budget Information Security Review

February 2026

Budget Information Security Review



© Crown copyright 2026

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at: www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at public.enquiries@hmtreasury.gov.uk

ISBN: 978-1-918417-20-3 PU: 3616

Contents

Chapter 1	Executive Summary	7
Chapter 2	Introduction	9
Chapter 3	The outcome and recommendations of the National Cyber Security Centre's investigation into recent OBR EFOs	11
Chapter 4	The steps HM Treasury is taking to tighten Budget information security and the Cabinet Office leak inquiry	16
Chapter 5	The approach to security and communications ahead of a Budget, including defining and applying those areas that are market sensitive and must remain confidential and what constitutes best practice in terms of any public commentary pre-Budget	21
Chapter 6	Annex A: Case studies	26
Chapter 7	Annex B: Screenshot of Reuters March 2025 alert logs	28

Chapter 1

Executive Summary

1.1 The National Cyber Security Centre (NCSC) agrees with the Office for Budget Responsibility's initial investigation that early access of the November 2025 Economic and fiscal outlook (EFO) was due to technical misconfiguration in the OBR's web publication process. Using information not available to the initial investigation the NCSC finds that early access was more widespread than originally reported. This more widespread access occurred after the initial point at which EFO content was released early in the media. After the first successful early access attempt, the original EFO was downloaded in full at least 24,701 times. The NCSC also agrees with the initial investigation that the same misconfiguration enabled early access to the March 2025 report. It finds that there were 16 successful accesses of the March EFO which all came from the same service provider. The NCSC was unable to investigate EFO publications before March 2025 because logs for EFOs before March 2025 were not available due to a 12-month retention policy.

1.2 The NCSC's two recommendations that are agreed by the OBR are being implemented: the March 2026 EFO will be published on GOV.UK by HM Treasury (HMT) on the OBR's behalf, pending a permanent move by the OBR to using the GOV.UK platform for market sensitive publications; and the Cabinet Secretary has commissioned a review of cross-government publishing in relation to sensitive information, both on and off of GOV.UK, to address the points raised in the report.

1.3 The Cabinet Office's leak inquiry into the Financial Times' 13 November 2025 article did not identify a source of the leak, but through its examination sets out how information security can be tightened, including a tightening of the compartments used to limit access to Budget information. It makes several recommendations that will be implemented in full ahead of the 2026 Budget.

1.4 HMT will tighten its internal Budget information security, including more restrictive IT controls, underpinned by the introduction of a new 'BUDGET - MARKET- SENSITIVE' classification for the most sensitive information, so that fewer officials will have access to sensitive information and the sharing of that information will be significantly restricted. The OBR will mirror these changes as applicable as well as taking other steps to strengthen information security for the wider body of forecast information.

1.5 The 'Macpherson Principles', which determine which information can and cannot be pre-briefed in public and/or with the media, will continue to apply. The Principles acknowledge that while most Budget information is not market sensitive, the economic and fiscal projections,

the fiscal judgement and individual tax rates, reliefs and allowances must not be pre-briefed.

1.6 It can be positively beneficial to consult and engage on policy ahead of announcement to deliver better, more informed, and more robust policies. In doing so this should be consistent with the Macpherson Principles. This was recently set out in the 2025 Tax Policy-Making Guidelines, whereby HMT and HMRC set out how to consult with stakeholders and tax professionals with the objective of making stronger tax policy.

1.7 The 'Parliament-first' principle is the subject of a recent Public Affairs and Constitutional Affairs Committee (PACAC) report, to which the Government will respond in due course.

Chapter 2

Introduction

2.1 A Review of Budget information security was commissioned in light of the events that occurred in the run up to the 2025 Budget Statement, in particular, on the day of the Budget, the contents of the Office for Budget Responsibility's (OBR) Economic and fiscal outlook (EFO) being accessed and then made publicly available before its intended release and the leak of information regarding Income Tax to the Financial Times (FT) on 13 November 2025, the story '*Starmer and Reeves drop proposal to raise income tax rates in Budget*'. Alongside a deeper investigation of recent EFO publications (mentioned below) and a working group to establish future OBR web publishing arrangements, the immediate investigation of that incident published in December 2025 recommended regular broader reviews of OBR IT and security arrangements – the first of which has been undertaken jointly with HMT as part of this Review.

2.2 The Budget Information Security Review is based on evidence from officials across HM Treasury (HMT), notably the teams that work most closely on preparation of the Budget, the Communications Team and the Chief Information Officer (CIO) as well as the Cabinet Office and the OBR. It also draws on the recommendations of the Cabinet Office-led, leak inquiry into the FT's 13 November 2025 story; and the National Cyber Security Centre's (NCSC) investigation into recent OBR EFO publications.

2.3 Advice on best practice has also been sought from The Bank of England on how a public organisation handles market sensitive information while operating under high levels of public scrutiny.

2.4 Further, a Panel including the Cabinet Secretary, the CEO of the National Cyber Security Centre, two HMT Non-Executive Directors, and a member of the OBR's Budget Responsibility Committee has provided HMT's Permanent Secretary with scrutiny and advice on the matters covered by this Review.

2.5 The Review report covers:

- The outcome and recommendations of the NCSC investigation;
- The outcome and recommendations of the Cabinet Office's leak inquiry;
- The steps HM Treasury is taking to tighten Budget information security;

- The approach to security and communications ahead of a Budget, including defining and applying those areas that are market sensitive and must remain confidential and what constitutes best practice in terms of any public commentary pre-Budget; and
- The work being taken forward by HMT, the OBR and The Bank of England on a protocol in the event of any future early releases of market sensitive information.

Chapter 3

The outcome and recommendations of the National Cyber Security Centre's investigation into recent OBR EFOs

3.1 On the day of the Budget, 26 November, at 11.35 – just under one hour before the Chancellor was due to speak, the content of the OBR's Economic and fiscal outlook (EFO) was able to be accessed erroneously. The OBR undertook an immediate investigation into this incident, overseen by its non-executive directors Baroness Sarah Hogg and Dame Susan Rice, which reported to the Chancellor and Treasury Select Committee (TSC) on 1 December¹. This investigation determined that the early access was caused by a technical misconfiguration into the OBR's web publication process. The report was unable to fully determine – in the time available – further information about the nature of the release and notably the extent of possible previous early access to EFOs before Budget 2025. It therefore recommended a further examination of this review, with expert support, was carried out. In December 2025 the government asked the NCSC to undertake this investigation.

3.2 The NCSC's findings are:

- The NCSC agrees with the OBR's initial report that early access of the November 2025 EFO was caused by a technical misconfiguration in the OBR's web publication process – as established by and reported on in the OBR's December 2025 initial review of the information breach;
- There appears to be nothing to evidence that the premature access to the report was the result of hostile cyber activity, connivance, or someone pressing the publication button too early. That the scale of access of the November 2025 EFO document was greater than found by the initial OBR investigation, because the NCSC has had

¹ https://obr.uk/docs/dlm_uploads/01122025-Investigation-into-November-2025-EFO-publication-error.pdf

access through the OBR to much more web log data than was initially available;

- That early access did occur to the March 2025 Spring Statement EFO, albeit on a much smaller scale than in November 2025;
- That because web log data is not held for more than 12 months, it is not possible for the NCSC to investigate whether there was early access of EFOs prior to March 2025.

November 2025 early access

3.3 The details of the NCSC's investigation are set out in the NCSC report that is published alongside this one. They are therefore not repeated here.

3.4 Rather, it is noted:

- The likely use of some kind of automation to repeatedly attempt to access the EFO early. 520 of the 534 attempts come from the same User Agent, 60-90 seconds apart, in three blocks of several hours each.
- Because the 520 attempts come from only 4 IP addresses, all of which are linked to the same Internet Service Provider, although it cannot be proved, a reasonable working hypothesis is that they originate or are linked to the same individual and/or organisation.
- After the first successful early access attempt, the original EFO was downloaded in full at least 24,701 times.
- The one or more individuals who secured early access to the EFO very likely used social media and messaging apps to spread word of the early access; since a significant number of the attempts to secure early access in the period following the initial early access come from clicking on weblink in a social media post and/or messaging app message, and all but 13 successful attempts occurred after EFO content had started being shared and broadcast by media outlets.

March 2025 early release

3.5 The full NCSC findings on the March 2025 access are published alongside this report. This Review notes that the report agrees with the OBR's initial investigation that the same misconfiguration enabled early access to the March 2025 report. It finds that there were 16 successful access of the March EFO. These requests to access the EFO come from IP addresses belonging to a single Internet Service Provider; and a messaging app was used to share the 'open' link to the EFO.

3.6 It is noted that the NCSC's report explains why it is not possible to identify to whom the IP addresses used in March or November 2025 belong. However, Reuters has publicly

stated that it did access the EFO early in March 2025². This is corroborated by publicly available information. Annex B is a screenshot of Reuters alerts from 26 March between 12:44 and 13:01. This HMT Review has found no evidence that these Reuters alerts came to the attention of the OBR, HMT or other news organisations, possibly because they were issued while the Chancellor was speaking, unlike in November 2025 when early access was achieved before the Chancellor began speaking.

3.7 The OBR's December 2025 report noted that there were some indications that an IP address associated with the March 2025 early access might be linked to accounts within UK government and/or other public authorities within the UK.

3.8 The NCSC's investigation has not found any evidence that any of the 16 IP addresses it has identified as requesting early access in March 2025 were linked to accounts within UK government and/or other public authorities.

3.9 Lastly, logs for EFOs before March 2025 have not been kept, and so the NCSC has not been able to determine whether early access took place for prior EFOs. It is noted that this means this possibility cannot be ruled out, although the NCSC investigation notes that a (latest January 2023) change to the OBR's web configuration is what appears to have first introduced the vulnerability used in March and November 2025. Furthermore, the OBR believes that its use of less predictable file path addresses prior to the October 2024 EFO means that early access prior to 2025 is less likely.

3.10 The NCSC's recommendations are:

- **That all future market sensitive OBR publications are made on GOV.UK**, because that platform is expressly designed for the regular publication of sensitive, embargoed information.
- **That all government departments and Arm's Length Bodies (ALBs) conduct a review to see if they hold and publish any market sensitive information outside of GOV.UK.** If they do, then these should be transferred to GOV.UK as a priority.

3.11 Both recommendations are accepted by HMT, the OBR and the Cabinet Office in full:

- The March 2026 EFO will be published on the OBR's behalf by HMT using GOV.UK, which is the platform HMT uses for all its publications.
- The Cabinet Secretary has commissioned a review of cross-government publishing in relation to sensitive information, both on and off of GOV.UK, to address the points raised in the report.

²Reuters first broke the news of early EFO access through an alert at 11.41 on 26 November 2025

3.12 The publication of the OBR's EFO on GOV.UK by HMT should not diminish the OBR's independence and will not give HMT access to any information ahead of time of which it is not already aware.

Other considerations in respect of the OBR's publications

3.13 The OBR will not publish the full forecast timetable ahead of the 2026 Spring Statement. The OBR will consider, ahead of Budget 2026, whether the current approach to publishing the timetable continues to contribute to transparency and stability as was intended when it was implemented in October 2022 following a recommendation by the OBR's then non-executive directors.

3.14 The OBR EFO is published on Budget Day to show the effects of new Government policy relative to a 'pre-measures' forecast. The pre-measures forecast for each Budget reflects changes in a significant number of variables since the previous EFO – such as the level of equities, gilt yields and prices, inflation and public sector borrowing outturn – as well as the impact of the OBR's judgements on the outlook for the economy and public finances, before any new policy measures are adopted, over the next five years.

3.15 The OBR shares a number of rounds of this pre-measures forecast with HMT in advance of the Budget. This gives the Chancellor a fiscal and economic baseline against which to judge the impact of the new policy measures they are considering – with the final pre-measures forecast providing the final baseline against which final policy decisions are taken.

3.16 The nature of the OBR's pre-measures forecast, and how it may change between each of the pre-measures forecast rounds, is often the subject of considerable debate and speculation by economic commentators and the media. Some of this debate is informed by public data – such as real time equities, gilt yields and prices or by ONS statistical releases such as for GDP, inflation and public sector borrowing – which has been published since the previous EFO. Indeed, a combination of new public data and expert forward judgements by economic experts can mean that the debate and speculation turns out to be reasonably accurate.

3.17 Consistent with the Macpherson Principles, the pre-measures forecast is not published in advance; nor are details of how the pre-measures forecast changed between each forecast round. As set out above, it has always been the case that the EFO sets out full details of the final pre-measures forecast, and this is very important for transparency, as by comparing this with the post-measures forecast, it illustrates the economic and fiscal impact of new government policy.

3.18 In November 2025, with the agreement of HMT, the OBR took the decision to publish some summary details of their earlier pre-measures forecasts rounds, after the full EFO had been published. Specifically, the OBR released information on the margin against the Chancellor's fiscal rules for the current budget and PSNFL (Public Sector Net Financial Liabilities) in each of the pre-measures forecasts. The OBR published

this information in agreement with HMT in response to intense speculation about the OBR's pre-measures forecasts, and took the form of a letter to the Chair of the TSC.

3.19 In some countries, such as the Netherlands, their equivalent fiscal forecaster publishes a forecast in advance of the country's Budget.

3.20 Some argue that doing this in the UK would increase transparency and contribute to debate about what policies the Government of the day should pursue in response to the forecast.

3.21 However, it would inevitably also generate considerable speculation about what the Government of the day was considering in response to forecast changes, particularly in periods where the forecasts change significantly from fiscal event to fiscal event. In turn, this could add to market uncertainty. It would also be in tension with the long-standing principle that governments should be afforded a private space in which they can consider a range of policy options.

3.22 Treasury's judgement is that the pre-measures forecasts should remain private to afford the government that private space. This judgement can be kept under review.

Chapter 4

The steps HM Treasury is taking to tighten Budget information security and the Cabinet Office leak inquiry

4.1 On 13 November 2025, the Financial Times ran a story ‘*Starmer and Reeves drop proposal to raise income tax rates in Budget*’. The Prime Minister and the Chancellor instigated a leak inquiry. This was run by the Cabinet Office’s Government Security Group as a thorough inquiry and has now reported.

4.2 All individuals and organisations in government who had access to the relevant information were in scope and it employed the full suite of investigative techniques available. This included interviews with more than sixty members of staff, ministers and special advisers across HMT, No.10 and the Cabinet Office. The inquiry did not identify the source or sources of the unauthorised disclosure. It did make the following recommendations:

- Whilst the security measures adopted by the Treasury around the sensitive Budget information relevant to this inquiry were in general followed appropriately, the use, and size, of named compartments around sensitive Budget information should be reviewed with a focus on the need-to-know principle;
- There should be a standard security induction brief for all staff across government working on sensitive Budget measures;
- The Treasury should consider how best to share information securely across departmental boundaries, including greater use of technical safeguards such as system-enforced access and sharing controls for the most sensitive measures.
- The Permanent Secretary to the Treasury should remind staff of their obligations under the relevant code to declare approaches from journalists with the communications director.

4.3 This report confirms that the recommendations will be implemented in full, as set out later in this section.

Budget information security in place at the time of Budget 2025

4.4 The Civil Service Code and contractual requirements on all staff at HMT, OBR and other departments mandate that information must be treated sensitively and that individuals “must not disclose official information without authority”.

4.5 The cornerstone of Budget information security is, and will remain, the need-to-know principle. In addition, the approach to Budget information security rests on HMT's broader suite of policies covering information security, IT usage and knowledge and information management (KIM).

4.6 The need-to-know principle for Budget information translates into the following, not exhaustive, measures:

- **All staff communications:** Before each fiscal event, the Strategy, Planning & Budget (SPB) Group holds a ‘launch event’ to which all HMT officials are invited, and which all officials likely to work on the Budget are encouraged to attend, at which the importance of maintaining information security, and the means of doing so, is set out. Further, the Permanent Secretary sends an information security email to the entire department reminding all staff of the importance of ensuring information security, and the consequences of not doing so.
- **Compartmentalisation:** HMT Directors are accountable for implementing a compartmentalisation policy for the policy areas that fall under their responsibility, so that only those officials working on these policies are involved. These officials are primarily those who work directly on the relevant policy area, though it will also include some officials in other parts of government that need to know about and be involved in the development of the policy – such as (for example) the officials working on related economic analysis, the methodology behind policy costings and/or advising on the deliverability of Budget measures.
- **Named lists:** Named lists are formally used, in addition to compartmentalisation, for especially sensitive parts of the Budget. These lists set out the only officials who can see particularly sensitive information and be involved in relevant policy development. Examples of information that are held on named-lists include the table of Budget policy decisions (the key analytical tool through which the Chancellor considers fiscal trade-offs associated with different policies), the OBR's economic and fiscal forecasts as they are received and, at most fiscal events, a number of the most sensitive measures to which project codenames are assigned.
- **Information technology (IT) measures:** The above measures are supported by several IT-enabled security measures in our Microsoft

ecosystem. HMT operates in line with the configuration expectations set out in Microsoft 365 Guidance for UK Government. This ensures that our handling of Budget-related information meets the standards jointly developed by Microsoft, Government Digital Service, Government Security Group, and the NCSC for departments working at the OFFICIAL classification tier in line with the need-to-know principle. HMT proactively manages access permissions to information, monitoring and logging changes to permissions and to live documents. For example, the Fiscal Event Database (FED – in effect the electronic database which supports HMT’s delivery of the Budget) is set up so that policy leads’ access is restricted to the measures on which they and their immediate teams are working, with access rights to a wider subsets of measures limited to officials where this is essential for their role.

4.7 HMT’s broader information security policies, on which the above measures rest, include:

- Alignment with the **Government Security Classifications Policy (GSCP)**, enabling consistent application of sensitivity labels and handling rules across HMT and departments;
- A **clear desk policy**, with regular security sweeps designed to prevent sensitive material being left on desks or in unlocked filing / storage solutions;
- Explicit rules that any media contact must be authorised by the Communications Team. A requirement to **inform the Communications Team of any contact with the media**;
- A requirement to **follow the Civil Service Code**, which includes the obligation to comply with the law and other public law requirements.

4.8 Distinct, but related, rules apply as to what can and cannot be pre-briefed outside the department. In 2013 – following the mistaken release of an embargoed briefing to the Evening Standard – a review was carried out by the then Permanent Secretary to HM Treasury Nick Macpherson. This review ended the practice of any substantive embargoed releases. It also examined what should and should not be kept confidential due to market sensitivity. These are the ‘Macpherson Principles’. They were set out in the 2013 Macpherson Review. This aspect of information security is considered in Chapter 5 of this report.

4.9 In general, the OBR applies and/or mirrors all the HMT Budget confidentiality and security guidance set out above, significantly aided by the move onto a segmented part of HMT’s shared IT system in December 2023. In some cases, minor adaptations are made in practically applying the guidance, reflecting the OBR’s role and size. A summary of the distinct features of the OBR’s approach is as follows:

4.9.1 All-staff communications are sent at the start of each fiscal event setting out information security protocols, including following any updated guidance or practices from HMT.

4.9.2 The OBR works closely with HMT to implement named lists for sensitive policy measures or parts of the Budget, led by OBR senior civil servants.

4.9.3 By contrast, the iterative and interconnected nature of the OBR's forecast means that forecast information needs to be widely available internally across the OBR team. Forecast material is shared internally via links to the OBR's internal file storage system rather than email attachments, meaning that files can't be accessed if accidentally forwarded.

4.9.4 The production of the forecast and certification of policy costings involves large amounts of information – such as economic determinants to feed into departmental tax and spending models, draft policy costing notes, and elements of EFO drafts for fact-checking – being shared between the OBR, HMT and other departments, typically via email attachments.

Changes to tighten HMT & OBR information security processes

4.10 The changes that follow look to address two potential areas of weakness:

- reducing information inadvertently shared; and
- reducing the risk of deliberate but unauthorised disclosure of information, noting it will never be possible to reduce this risk to zero.

4.11 The principal changes, which will be introduced ahead of Budget 2026, are:

- A set of mandatory embedded protection actions within the IT systems to restrict the extent to which Budget material can be shared, including across departmental boundaries. Measures will include preventing the sending of attachments; limiting access to named lists and restricting the functionality for those accessing information to print or download; and with the ability to monitor and record access;
- Linking these protections to the introduction of a new 'BUDGET - MARKET SENSITIVE' sensitivity label for the most sensitive categories of Budget and forecast information where HMT and OBR use named lists;
- Cutting back the numbers of officials who can routinely access the most sensitive information. For example: reducing the numbers of officials with awareness of measures on named lists, while increasing the numbers of measures that are subject to these protections; and

reducing the numbers of officials who can access the contents of OBR forecast rounds and the table of Budget policy decisions.

4.11.1 In addition to implementing all of the above, the further changes that the OBR will make ahead of Budget 2026 are:

- Introducing an “OBR only” sensitivity label, which prevents emails from being shared outside the OBR, to further protect internal OBR sharing of forecast and policy information as the forecast is compiled.
- Improving the security around the large volume of less sensitive forecast and policy information that is shared between the OBR and HMT/other forecasting departments by implementing security labels and/or shared file storage areas which bound the information to the teams or departments involved.

4.12 When deciding exactly how to tighten Budget information security, a balance must be struck between ever tighter security and the benefit to good policy-making of proper sharing of information within HMT and between HMT and other parts of government. For example, HMT’s published distributional analysis of Budget measures requires those officials producing the distributional analysis to have sight of the full range of relevant measures. Likewise, officials and ministers will seek to understand the cumulative effect of all of a Budget’s measures on particular sectors of the economy, and how they respond (for example) to stakeholder representations.

4.13 The Review believes that while the information security tightening described above will make some elements of cross-HMT and cross-government collaboration more onerous – and will certainly feel much more onerous to some officials – they strike the balance between a necessary tightening of information security and effective policy-making.

Chapter 5

The approach to security and communications ahead of a Budget

Including defining and applying those areas that are market sensitive and must remain confidential and what constitutes best practice in terms of any public commentary pre-Budget.

5.1 It is important that the Government can handle market sensitive information carefully to minimise the prospect of unauthorised disclosures of information. There is more that can be done to ensure this is the case. The distinction between what is market sensitive and should not be communicated, and what is not, was the subject of the 2013 [‘Review into the pre-release of Budget information’](#) (henceforth, ‘the Macpherson Review’).

The 2013 Macpherson Review

5.2 The [Macpherson Review](#) set out, and explained, the rules that have ever since applied to how Budget information is communicated by HMT.

5.3 Its keystone is:

5.4 “a ban on the pre-release of the core of the Budget (and Autumn Statement), that is: the economic and fiscal projections, the fiscal judgement and individual tax rates, reliefs and allowances.”

5.5 The Macpherson Review also noted several important pieces of context at the time, including:

- A steady evolution in HMT’s Budget communication practice from the late 1990s onwards, in part reflecting the evolving media landscape, in part reflecting that numerous organisations published economic and fiscal forecasts;
- That Budget leaks are not new. The Review refers to an example in 1996 where a newspaper accessed much of the Budget, while the Review itself was a response to an inadvertent leak of information pre-briefed to another publication;

- That, to quote, “the vast majority of Budget measures were not market sensitive and had often been trailed in the Pre-Budget Statement (or more recently the Autumn Statement)”;
- Changes to the security classification applied to Budget information within HMT, the Review noting that by 2013, it was two classification levels down from the 1990s;
- The use of information pre-release arrangements by a number of government departments, with the objective of enabling sensitive information to be communicated promptly and accurately, thereby minimising the risks, including to market volatility, of inaccurate reporting of information; and
- Furthermore, ministers in all administrations have, entirely reasonably, made economic policy announcements and commented on economic policy and developments multiple times a year, including in the run up to fiscal events. Indeed, for more than a decade, starting in 2010, the Chancellor of the Exchequer of the day would routinely be interviewed on the BBC’s flagship political programme just days before delivering their Budget to Parliament. This is considered in greater detail at 5.15 onwards.

How the external environment has evolved since 2013

5.6 Some of the contextual elements identified by the Macpherson Review have continued to evolve, some at pace:

5.7 The change to an increasingly online business model for media organisations has been accompanied by a growth in Budget-related content – particularly personal finance matters – often speculative in nature.

5.8 The rapid growth of social media and other online platforms that offers individuals and organisations outside the more closely regulated media platforms and organisations the ability to speculate and share information instantly

5.9 The high-profile publication of high quality economic and financial forecasts by expert external organisations in the run up to the Budget, remains a significant element of the context in which HMT operates³. These are an important contribution to economic policy debate, and transparency, in the UK.

5.10 This operating environment requires HMT Ministers, media special advisers and Civil Service press officials to make daily, sometimes hourly, judgements on media stories and think tank

³ The British Chamber of Commerce (BCC), Centre for Economics and Business Research (CEBR), Institute for Fiscal Studies (IFS), International Monetary Fund (IMF), National Institute of Economic and Social Research (NIESR), the Organisation for Economic Cooperation and Development (OECD) and The Resolution Foundation (RF) all produce such forecasts; while several of these, alongside organisations such as the Institute for Public Policy Research (IPPR) and Joseph Rowntree Foundation (JRF) produce their own analysis of other important elements of the Budget, such as distributional analysis of Budget policy measures.

publications and commentary being put to Communications for comment in the run up to a Budget. These are some of the several reasons why Budget speculation, however well-informed, will remain a major – and increasing – feature of the run-in to fiscal events in the future.

HMT & stakeholders: the Budget policy-making process

5.11 The importance of engaging with stakeholders on policy-making has been recognised by successive governments. Tax policy-making principles were first published in 2010⁴. The most recent set of principles were published in June 2025⁵, which sets out that “the government will consult on tax policy where it deems it necessary to do so”, with any consultation “precise, targeted and only [seeking] information that is genuinely needed”. A “key principle that underpins the government’s approach to tax policy making is robust engagement with interested groups”.

5.12 A consistent theme since the 2010 publication has been the use of regular consultation with tax professionals and policy stakeholders on all stages of tax policy development. It can be positively beneficial to consult and engage on policy ahead of announcement to deliver better, more informed, and more robust policies.

5.13 The main reason why HMT consults on tax policy development is to make better policy and to provide stability and predictability to taxpayers. Case studies from previous Budgets to illustrate this point can be found in Annex A. One consequence of this approach is that, for many measures being considered ahead of a Budget, knowledge of what ministers are considering extends outside government. Therefore, the media may become aware through contacts outside of government of some of these considerations.

5.14 This is an inevitable consequence of a more transparent approach to policy development; and is part of the explanation as to why Budget policy debate and speculation will remain a feature going forward. In doing so this should be consistent with the Macpherson Principles.

External engagement: pre-briefing

5.15 Alongside external consultation of the kind described above, successive governments have reasonably chosen to make non-market sensitive Budget announcements, as well as explaining their approach to economic and fiscal policy, in the run up to Budget day.

5.16 This has on occasion prompted debate about the ‘Parliament first’ principle. But this debate goes much wider than just Budget-related matters. The operationalisation of the long-standing convention that major policy announcements should be made first to

⁴ [House of Commons - Principles of tax policy - Treasury](#)

⁵ www.gov.uk/government/publications/tax-policy-making-principles/tax-policy-making-principles

Parliament has been the subject of a recent PACAC report⁶. The Government will respond to the report in due course.

5.17 What is not in doubt is that it is wholly proper for ministers to make announcements on matters such as new public spending decisions, or offer commentary or answer questions about the direction of travel of a particular policy area, or their approach to economic and fiscal policy, throughout the year. The example of the pre-Budget flagship BBC political interviews referred to previously is one of innumerable examples that could be given.

5.18 Nor do the Macpherson Principles prevent ministers from making market sensitive economic and tax announcements outside of Budgets – such as in the recent case of changes to agricultural property relief and business property relief in December 2025. The Principles are designed to prevent anyone gaining an advantage from privileged information that could bestow a financial or commercial advantage.

Changes to external handling of market sensitive information:

5.19 It is unrealistic and sub-optimal to rule out all briefing or commentary on a Budget. Rather, any briefing must be alive to not releasing market sensitive information. As such, the Macpherson Principles apply. We have looked again at whether these Principles should be updated in light of the increased speculation that now is pervasive, but conclude that we should continue to apply them in full.

5.20 This Review therefore confirms that:

- The Macpherson Principles continue to apply.
- The Macpherson Principles will continue to be communicated to all HMT officials ahead of each fiscal event as part of the Permanent Secretary's All Staff email. In addition, all Press Officers and Special Advisers will have to confirm in writing their understanding of, and adherence to, the Principles.
- Any breach of the Principles will be treated as serious or gross misconduct.
- It remains good policy practice to look to consult on measures ahead of announcement. As such, HMT will continue to follow its Tax Policy Making Principles. In doing so, this should be consistent with the Macpherson Principles.

The work being taken forward by HMT, the OBR and The Bank of England on a protocol in the event of any future early releases of market sensitive information

5.21 The early release of the November 2025 EFO also brings out the need for the OBR and HMT to have a contingency plan for this kind of

⁶ [PACAC's January 2026 report on Ministerial Statements and the Ministerial Code](#)

event; since future breaches of information security, whatever their origin, cannot be ruled out.

5.22 HMT and the OBR will work in partnership with The Bank of England to establish a protocol for such an eventuality. This work will draw on The Bank of England's current contingency arrangements in the event that, for example, information about a monetary policy decision becomes public in an unplanned manner.

5.23 The first steps in this work are to identify which sort of information should be in scope and to engage with market participants to identify the most useful mechanisms which the three institutions could use in response to a future information breach. A likely guiding principle of the work is to avoid as far as possible tradeable information being known to a subset of market participants, knowledge which could give those participants a commercial advantage.

5.24 The objective is to have the protocol in place well before this year's Budget.

Chapter 6

Annex A: Case studies

6.1 HM Treasury consults on tax policy development to make better policy and to provide stability and predictability to taxpayers. The following two case studies illustrate the application of different ways of engaging externally – including when designing market sensitive tax changes.

Gambling tax

6.2 In Spring 2025, HM Treasury published a consultation exploring options including proposals to consolidate three existing remote (online) gambling taxes – remote gaming duty, general betting duty, and pool betting duty – into a single duty. As part of the consultation process, HM Treasury also undertook targeted engagement such as stakeholder meetings and roundtables, including with the gambling sector, which was designed to gather input on issues including tax design and the potential impacts of reform.

6.3 The consultation broadened HM Treasury's evidence base by capturing a range of views from across a diverse array of stakeholders. Crucially, this included stakeholders highlighting distinct differences in risk profiles and social harms between betting and gaming, underpinning arguments for differential treatment within any new tax regime.

6.4 This evidence informed the Ministers' consideration of risks, benefits, and potential impacts of the reform. This contributed to the development to the broader reform package announced at Budget 2025.

6.5 Alongside the Budget announcement, HM Treasury published a government response to the consultation, setting out details of the package alongside responses to the issues raised during the consultation process. Continued engagement throughout the policy development process was aimed to ensure reforms were evidence based and reflected real-world impacts.

Carbon Border Adjustment Mechanism

6.6 The Carbon Border Adjustment Mechanism (CBAM) is a landmark climate policy designed to equalise the carbon price between domestically-produced goods and imports, giving domestic industry the confidence to invest in decarbonisation, knowing their efforts will not be undermined. The policy is market sensitive and directly impacts

a limited number of sectors (aluminium, cement, fertiliser, hydrogen and iron & steel).

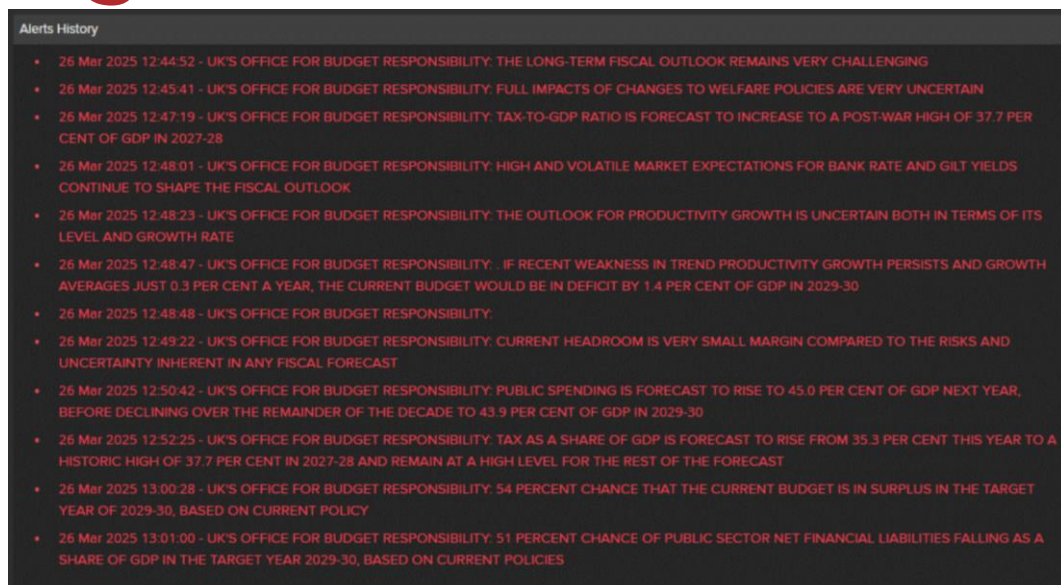
6.7 Given the complexity of the policy, it has been subject to significant external engagement and formal consultation over a number of years. The previous government undertook an 'Addressing carbon leakage risk to support decarbonisation' consultation in 2023. The [current] government published a response to a further policy consultation in 2024, and draft primary legislation for CBAM was published in April 2025 for technical consultation.

6.8 The consultations over a period of time built HMT's understanding of policy design and implementation, including defining sectoral scope, calculating liability and minimising the administrative burden. This contributed directly to the announcements at Budget 2025 for the 2027 introduction of a CBAM.

6.9 These two case studies illustrate how appropriate open engagement, transparency, and thoughtful consultation underpin higher quality outcomes in tax policy and deliver on government objectives.

Chapter 7

Annex B: Screenshot of Reuters March 2025 alert logs



HM Treasury contacts

This document can be downloaded from www.gov.uk

If you require this information in an alternative format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 5000

Email: public.enquiries@hmtreasury.gov.uk