A Critical Appraisal of Data Centre Development in England and Wales

Environmental Sustainability, Infrastructure Resilience, Digital Sovereignty and Public Trust.

So many questions and so few answers.

Dennis Clarke

Contents

Abstract....4
Executive Summary....6
1. Introduction....8
2. Planning Policy in England and Wales....9
England....9
Wales....9
3. The Economic Case....11
Employment and the Long-Term Jobs Question....11
International Profits and the Question of Tax....13
The Scale and Deliverability of Proposed Investment....14
Data Retention and the Question of Necessity....17
4. Electricity Demand and Energy Infrastructure....19
5. Water Use and Cooling Technologies....20
Kept from the public: the EU's reporting rules for data centres....21
Local interest in water supplies....25
6. Carbon Emissions and Climate Change....30
7. Energy-from-Waste and Incinerator-Related Power....33
Waste heat: a resource the planning system has not yet asked about....33
Food security, glasshouses and water reuse....35
Case study: Cardiff East Park and Ride....36
8. Local Environmental Effects....40
Chemicals of concern in construction and operation, including PFAS 'forever chemicals'....40
9. Digital Sovereignty, Jurisdiction and Public Trust....49
10. International Data Transfers and Jurisdictional Complexity....50
11. The CLOUD Act and International Governance....51
12. Public-Sector Data and National Sovereignty....52
Recent experience: Palantir in the UK public sector, and the United States 'DOGE' episode....52
Control of computing power, not only of data....56
13. Regulatory Stability and International Confidence....60
Sovereignty by dependence: a discussion point....60
14. Resilience, Backup and Systemic Risk....65
15. Regional Concentration and Proliferation Effects....66

London and Slough....66
South Wales....67
16. Bro Tathan: Public Land, a US Operator and Unresolved Governance Questions....69
What the screening file shows (October 2026)....70
17. Artificial Intelligence: Warnings, Uncertainty and the Precautionary Principle....73
Beyond loss of control: deliberate misuse risks....77
Rogue and hostile states: a harder threat to detect than a nuclear programme....80
Software reliability: building on tools that may not be bug-free....83
An independent national assessment: the Alan Turing Institute (September 2026)....85
The Government's own position: understanding admitted, safeguards deferred....88
18. Whose problem is this?....92
19. Public Policy Questions....93
20. Practical Assessment Framework....96

Abstract

Data centres have become essential infrastructure for modern society, we are told. It has been described as the fourth industrial revolution.

Data Centres support cloud computing, financial services, telecommunications, healthcare, government administration, scientific research and artificial intelligence (AI). In September 2024, the UK Government designated data infrastructure as Critical National Infrastructure (CNI) in England, reflecting its growing importance to economic activity, public services and national resilience.[1,2]

At the same time, the rapid expansion of data-centre development has prompted debate concerning electricity demand, water consumption, carbon emissions, land use, data governance, digital sovereignty and resilience. While many of these issues can be measured through technical analysis, others involve broader questions of public policy and governance.

This article proposes a framework for assessing major data-centre developments in England and Wales. It neither advocates unrestricted expansion nor opposes development in principle. Instead, it seeks to identify many principal environmental, technical, legal and societal considerations that should inform decision-making and the public.

The document asks questions where no answers have been found. It is constructed on the Precautionary Principle.

It was at the Asilomar Conference on Beneficial AI in 2017 that perhaps the most important point was stressed. There was a danger identified and discussed that the development of AI might progress so quickly that society might not be able to adjust. It does feel like we are rushing headlong into something that we do not understand.

The opening lines to Kipling's A Smuggler's Song include the best reason for getting

involved, asking questions, test the answers until you are content with them. There are many ways for a lie to be told or to be assumed.

> *If you wake at midnight, and hear a horse's feet,*
> *Don't go drawing back the blind, or looking in the street,*
> *Them that ask no questions isn't told a lie.*
> *Watch the wall, my darling, while the Gentlemen go by!*

Ask now, do not wait to complain later.

---

[1] Department for Science, Innovation and Technology, Designation of UK Data Infrastructure as Critical National Infrastructure, Written Ministerial Statement HCWS89 (12 September 2024). https://questions-statements.parliament.uk/written-statements/detail/2024-09-12/HCWS89

[2] Department for Science, Innovation and Technology, Data Centres to be Given Massive Boost and Protections from Cyber Criminals and IT Blackouts (12 September 2024). https://www.gov.uk/government/news/data-centres-to-be-given-massive-boost-and-protections-from-cyber-criminals-and-it-blackouts

Executive Summary

Data centres are the industrial infrastructure of the digital age. Every online search, streamed film, mobile phone transaction, cloud document, AI query and digital healthcare record depends upon them. Government policy increasingly recognises their importance to economic growth and national resilience.[3,4,5]

However, data centres are not impact-free.

Large facilities can require substantial supplies of electricity, may consume significant quantities of water, generate noise, create demands on infrastructure networks and raise questions concerning long-term control of information.

Concerns have also emerged regarding concentration of infrastructure, resilience to future climate conditions and the growing importance of a relatively small number of global cloud-service providers.[6,7,8,9,10]

Several further issues addressed later in this appraisal deserve particular attention:

- the uncertain long-term employment case for individual developments in an era of increasing automation;
- the governance questions raised when a public body simultaneously acts as landowner, promoter and regulator of major digital infrastructure;
- whether the international corporate groups operating these facilities pay a fair share of UK tax on the profits they help to generate;
- whether the very large sums of investment now being announced are realistically deliverable;
- what happens to funding for necessary infrastructure upgrades if headline figures do not already include their cost;

[3] See n 1 above (DSIT, WMS HCWS89).
[4] See n 2 above (DSIT press notice).
[5] House of Commons Library, Data Centres: Planning Policy, Sustainability and Resilience, Research Briefing CBP-10315 (27 May 2026). https://commonslibrary.parliament.uk/research-briefings/cbp-10315/
[6] Ibid.
[7] Department for Energy Security and Net Zero, Data Centre Electricity Consumption in Great Britain, 2020–2024 (Official Statistics in Development, June 2026). https://assets.publishing.service.gov.uk/media/6a3e9f25da47783d87723bf2/Data_centre_electricity_consumption_in_Great_Britain__2020_to_2024.pdf
[8] techUK, Understanding Data Centre Water Use in England (2025). https://www.techuk.org/resource/techuk-report-understanding-data-centre-water-use-in-england.html
[9] Water Research Centre (WRc), Data Centre Water Use Report (2026). https://h2oglobalnews.com/data-centre-water-use-report-england/
[10] House of Commons Environmental Audit Committee, Risks and Opportunities to the Sustainability of Data Centres in the UK (Inquiry, 2026). https://committees.parliament.uk/work/9651/risks-and-opportunities-to-the-sustainability-of-data-centres-in-the-uk/

- the warnings some of those building the most advanced AI systems have themselves issued about the technology's risks, both from AI acting on its own initiative and from deliberate misuse by a person or group;
- the difficulty of detecting a hostile state developing dangerous AI capability, compared with the greater visibility of a nuclear weapons programme;
- the possibility that a small, difficult-to-track team could achieve meaningful capability;
- whether AI systems can be relied upon as more dependable tools than the conventional software that already, even from the most resourced developers, requires frequent urgent patching; and
- whether the PFAS ('forever chemicals') used in some data-centre fire-suppression and cooling systems pose an environmental and decommissioning risk that has, on the evidence available, gone largely unaddressed by UK and Welsh regulators to date.

The key question is therefore not whether data centres should exist, but whether individual developments can demonstrate that environmental, social and governance issues have been addressed appropriately.

1. Introduction

Few forms of infrastructure have become as important to modern life as data centres, yet few remain as poorly understood outside specialist circles.

Historically, data centres were primarily associated with business computing and corporate record management. Today they underpin cloud computing, internet services, online retailing, financial transactions, telecommunications, scientific research and increasingly artificial intelligence. The UK Government has recognised this importance by designating data infrastructure as part of the nation's Critical National Infrastructure.[11,12]

Demand for computing capacity is expected to increase significantly during the coming decade. Government analysis and Parliamentary scrutiny suggest substantial growth in UK data-centre requirements, particularly as AI technologies become more widely adopted.[13,14]

The challenge is how to accommodate that growth while ensuring developments remain environmentally sustainable, socially acceptable and institutionally resilient.

If, when, decisions have to be taken to prioritise who receives electricity or water, are the datacentres prioritised over people. No doubt contracts exist that can be disclosed to set out what obligations have already been agreed.

[11] See n 1 above (DSIT, WMS HCWS89).
[12] See n 2 above (DSIT press notice).
[13] See n 5 above (HoC Library, CBP-10315).
[14] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).

2. Planning Policy in England and Wales

England

Planning policy in England has become increasingly supportive of data-centre development. Recent national planning reforms have recognised the importance of digital infrastructure and encouraged local authorities to consider provision for future data-centre requirements.[15]

Supporters argue that these reforms are necessary if the United Kingdom is to remain competitive in artificial intelligence, cloud computing and advanced digital services.[16,17]

Critics argue that national policy support should not diminish scrutiny of environmental and local impacts.

Both perspectives have merit.

Wales

Wales has taken a somewhat different approach to date.

Data-centre proposals are primarily considered through Planning Policy Wales, Future Wales, Technical Advice Notes and wider sustainable-development objectives rather than through a dedicated data-centre policy framework.[18]

Recent Welsh policy developments have sought to streamline infrastructure decision-making while maintaining emphasis upon sustainable development, community benefit and place-making.[19,20]

The distinction between England and Wales should not be overstated. Both administrations recognise the importance of digital infrastructure. The principal difference lies in policy emphasis and institutional context rather than strategic direction.[21,22]

That said, a critical appraisal should not understate the practical consequences of the different approaches taken. In England, the classification of data infrastructure as Critical National Infrastructure, reform

---

[15] Browne Jacobson, NPPF 2026 Amendments: Data Centres and On-Site Energy Generation (2026), summarising National Planning Policy Framework reforms concerning data-centre and AI infrastructure planning (2024–2026). https://www.brownejacobson.com/insights/nppf-2026-amendments-browne-jacobson-response/data-centres-and-on-site-energy-generation

[16] See n 5 above (HoC Library, CBP-10315).

[17] See n 15 above (Browne Jacobson, NPPF 2026 Amendments).

[18] Welsh Government, Planning Policy Wales (Edition 12, updated July 2024). https://www.gov.wales/planning-policy-wales

[19] Ibid.

[20] Senedd Research, Data Centres in Wales: How Will Wales Manage a Rapidly Growing Industry? (July 2026). https://research.senedd.wales/research-articles/data-centres-in-wales-how-will-wales-manage-a-rapidly-growing-industry/

[21] See n 18 above (Welsh Government, Planning Policy Wales).

[22] See n 20 above (Senedd Research, Data Centres in Wales).

of the National Planning Policy Framework and the extension of the Nationally Significant Infrastructure Projects regime have together tended to move decision-making on the largest data-centre schemes toward central government, narrowing the discretion available to local planning authorities.[23]

Wales has adopted no equivalent dedicated framework. Data-centre proposals continue to be determined under general sustainable-development and place-making policy, with the Welsh Government's principal lever being its Ministerial power to issue a holding directive or call in an individual application - as it did in August 2026 in respect of a proposed data centre at a Cardiff park-and-ride site, pending a decision on whether to determine the application itself.[24]

Each approach carries trade-offs.

England's more centralised model offers greater consistency and speed for developers but reduces the scope for local scrutiny of individual schemes.

Wales's more general, policy-led approach preserves local decision-making and flexibility but risks unpredictability, since outcomes may turn on whether Ministers choose to intervene in a particular case rather than on a published, generally applicable framework.

Industry commentators have specifically identified the absence of a dedicated Welsh data-centre strategy as an outstanding gap, notwithstanding Wales's evident ambitions in this sector.[25,26] A clearer, published Welsh Government policy statement - setting out how proposals will be assessed, how any conflict between the Welsh Government's roles as landowner, promoter and regulator will be managed, and how host communities can expect to benefit - would reduce this unpredictability without requiring wholesale adoption of the English model.

[23] See n 15 above (Browne Jacobson, NPPF 2026 Amendments).
[24] Britbrief, Welsh Government Could Decide Cardiff Data Centre Plans After Holding Directive (August 2026). https://britbrief.co.uk/business/property/welsh-government-may-decide-cardiff-data-centre-plans.html
[25] Business News Wales, The Rise of Data Centres in Wales (2026). https://businessnewswales.com/the-rise-of-data-centres-in-wales/
[26] DataCenterDynamics, Silicon Valleys: How Wales Aims to Become a Data Center Hub (analysis, 2026). https://www.datacenterdynamics.com/en/analysis/silicon-valleys-how-wales-became-a-data-center-hub/

3. The Economic Case

The economic case for data-centre investment is substantial.

Modern economies depend upon digital infrastructure. Data centres support financial services, telecommunications, scientific research, cloud computing, public administration and AI-enabled technologies.[27]

There is also a strategic argument. Domestic digital infrastructure may improve resilience, reduce dependence upon overseas capacity and support national economic development.[28,29,30]

Nevertheless, economic claims should be examined carefully.

Although construction phases can generate substantial temporary employment, operational facilities are often highly automated and may support relatively small permanent workforces compared with the scale of the infrastructure involved.[31,32]

Planning decisions should therefore distinguish clearly between construction employment, long-term jobs and wider economic benefits.

Employment and the Long-Term Jobs Question

This distinction deserves closer attention than it typically receives at the application stage.

Hyperscale data-centre campuses can occupy sites of considerable scale - in some cases land otherwise allocated in local development plans for general employment use - while supporting comparatively modest permanent workforces once construction is complete: one recent Welsh example is put at around 120 permanent jobs.[33]

One independent analysis of the wider UK sector has gone further, questioning whether headline job-creation figures quoted by developers at the application stage are consistently matched by actual long-term operational employment once facilities are operational.[34]

At the same time, UK-wide projections point toward substantial sector growth in employment terms. techUK has estimated that data centres currently support around 43,500 jobs across the UK, with the potential for this to rise significantly - some analysis suggests towards 100,000 or more

---

[27] See n 5 above (HoC Library, CBP-10315).
[28] See n 1 above (DSIT, WMS HCWS89).
[29] See n 2 above (DSIT press notice).
[30] See n 5 above (HoC Library, CBP-10315).
[31] See n 5 above (HoC Library, CBP-10315).
[32] See n 20 above (Senedd Research, Data Centres in Wales).
[33] See n 26 above (DCD, Silicon Valleys).
[34] European Powell (Substack), Consent Not Required: How Big Tech Is Rewriting British Law to Build Its Data Empire Beyond Democratic Reach (2026) — an independent critical commentary; cited here for its characterisation of disputed job-creation claims, not as a neutral primary source. https://europeanpowell.substack.com/p/consent-not-required-how-big-tech

by 2035 as capacity expands, and higher still once workforce turnover and retirement are taken into account.[35] These figures are not necessarily inconsistent with modest site-level headcounts: they are aggregated across a growing number of facilities nationally, and a meaningful share reflects construction, supply-chain and specialist technical roles rather than steady-state operational staffing at any single campus.

Planning authorities and communities should therefore be cautious about treating national sector-level projections as a guide to the number of long-term jobs any particular development will support locally.

A further, more difficult question concerns the effect of increasing artificial intelligence adoption on data-centre employment itself. On one view, greater automation of monitoring, predictive maintenance and remote operations management is likely further to reduce the already modest steady-state headcount required to run a large facility over its operational life, which may extend to twenty years or more.

On another view, the same trend may generate new categories of specialist employment - in AI infrastructure engineering, data-centre design and grid integration - that at least partially offset losses elsewhere, and commentators have separately identified a persistent skills shortage in the sector, with close to half of the existing technical workforce expected to reach retirement age by 2030.[36]

These two observations are not easily reconciled, and the honest position is that the net long-term employment effect of AI-driven automation on data-centre operations remains genuinely uncertain - the jury is still out.

This uncertainty is not, in itself, a reason to resist development, but it is a reason for government - in both Cardiff and London - to be considerably more explicit than it has been to date. Neither the UK Government's National Planning Policy Framework reforms nor Welsh planning guidance currently offers planning authorities clear, evidence-based guidance on realistic long-term employment expectations for data-centre developments, as distinct from construction-phase activity.

Given the scale of land these developments can occupy - often on sites otherwise capable of accommodating higher-employment-density uses - government should set out a considered, updated view of how AI-driven automation is expected to affect long-term staffing levels at such facilities, so that the employment case for individual proposals can be weighed accurately, rather than assumed, against the alternative uses of the land involved.

[35] Data Centre Review, The Data Centre Boom Will Stall Without a Skills Plan (April 2026). https://datacentrereview.com/2026/04/the-data-centre-boom-will-stall-without-a-skills-plan/
[36] Ibid.

International Profits and the Question of Tax

A separate question, distinct from the employment case addressed above, is whether the United Kingdom and Wales secure a fair fiscal return from data centre development once these facilities are built and operating.

Many of the international groups building data centres at scale in England and Wales are large multinationals capable of arranging their corporate affairs so that profits attributable to UK operations are recognised, for tax purposes, in other and more lightly taxed jurisdictions. The Digital Services Tax, often assumed to reach large technology companies generally, does not address this: it applies only to revenue from social media services, internet search engines and online marketplaces, and has no application to cloud computing, data storage or the underlying infrastructure services that a data centre supplies.[37,38]

The OECD's Pillar Two reforms, transposed into UK law as the Multinational Top-up Tax, were intended to guarantee a minimum 15% effective tax rate on the profits of large multinational groups wherever they are booked, closing off much of the incentive to shift profits to low-tax jurisdictions.

In practice, a 'side-by-side' agreement reached in January 2026 exempted US-headquartered groups from Pillar Two calculations, and HM Revenue and Customs has told the House of Commons Committee of Public Accounts that this exemption will reduce the UK's expected annual benefit from Pillar Two by around £600 million, down to about £1.6 billion. Given that most of the large hyperscale operators active in the Welsh and English data centre market are US-headquartered, this carve-out is directly relevant to the sector under discussion in this appraisal.

The Committee's report, published on 10 July 2026, went further, recording that international tax risks - including businesses artificially shifting profits to lower-tax jurisdictions - account for some £21 billion of the tax currently under investigation by HMRC in relation to large businesses generally, and concluding that the scale of risk posed by large multinationals diverting profits across borders remains significant even with the new minimum tax rate in place.[39]

A related, more local, fiscal question concerns business rates. Data centres are valued for rating purposes on a basis that depends heavily on technical assumptions about plant and machinery, and on whether unequipped 'white space' awaiting tenant fit-out is rateable at all - a point of genuine legal

---

[37] Finance Act 2020, Part 2 (ss.39-72), especially s.43(2), defining "digital services activity" for Digital Services Tax purposes as limited to social media services, internet search engines and online marketplaces. https://www.legislation.gov.uk/ukpga/2020/14/part/2

[38] House of Commons Library, Digital Services Tax, CBP-8719 (2026). https://commonslibrary.parliament.uk/research-briefings/cbp-8719/

[39] House of Commons Committee of Public Accounts, Large Business Tax Compliance, HC 86 (10 July 2026). https://publications.parliament.uk/pa/cm5902/cmselect/cmpubacc/86/report.html

uncertainty until the Upper Tribunal's 2021 decision in Ricketts (VO) v Cyxtera Technology UK Ltd confirmed that such space could, on the facts of that case, be treated as non-domestic property in its own right.

The valuation of large, technically complex data centre premises accordingly remains more contestable, and less transparent to an outside observer, than the valuation of most other commercial premises, which in turn affects the local business rates revenue such sites generate for Welsh and English authorities.[40,41]

Notably, when the Senedd's own research service examined the growth of the data centre sector in Wales, its analysis addressed investment, employment claims, energy, water and grid capacity at length, but did not extend to any assessment of the tax or business rates return to Wales from this investment.[42]

This appraisal does not attempt to resolve these questions, but it suggests that government should be pressed for clarity in the same way as on the employment and AI questions raised elsewhere in this paper. A written question that might be put to the Senedd or a Westminster MP is:

> *'What assessment has [the Treasury / the Welsh Government] made of the corporation tax and business rates revenue forecast to be collected from data centre operators in [the UK / Wales] over the next five years, and what steps are being taken to ensure that international operators account for profits attributable to their UK data centre operations in the UK rather than in lower-tax jurisdictions?'*

No answer to a question in these terms currently exists, and no Freedom of Information request on this specific point appears to have been made via WhatDoTheyKnow.

The Scale and Deliverability of Proposed Investment

The scale of capital committed to AI-related data-centre infrastructure by the largest technology companies has increased sharply.

Combined 2026 capital-expenditure guidance from Microsoft, Alphabet (Google's parent company), Meta and Amazon reached approximately $725 billion, up from around $410 billion in 2025, with Microsoft and Alphabet each guiding to approximately $190 billion and Amazon raising its guidance to approximately $220 billion.

---

[40] Ricketts (Valuation Officer) v Cyxtera Technology UK Ltd [2021] UKUT 0265 (LC). https://landschamber.decisions.tribunals.gov.uk/judgmentfiles/j1755/LC-2019-611.pdf

[41] Browne Jacobson, Data Centres and Business Rates: What Investors Miss (2026). https://www.brownejacobson.com/insights/data-centres-and-business-rates-tax-on-megawatts

[42] Senedd Research, Data Centres in Wales: How Will Wales Manage a Rapidly Growing Industry? (2026). https://research.senedd.wales/research-articles/data-centres-in-wales-how-will-wales-manage-a-rapidly-growing-industry/

Separately, the Stargate joint venture involving OpenAI, SoftBank and Oracle, first announced in January 2025 at a headline $500 billion over four years, had by September 2025 committed sites totalling almost 7 gigawatts of capacity and over $400 billion of confirmed investment.[43,44,45,46,47]

These sums are not spread evenly. They tend to show the speed with which decisions are made which must be unique and possibly dangerous.

Announcements to date concentrate heavily on the United States, the Gulf states and a small number of other jurisdictions, including Wales.

Microsoft and the Emirati company G42 announced a further $15.2 billion of UAE data-centre investment in November 2025, part of a wider pattern of Gulf-region commitments that analysts have described as a 'trillion-dollar bet', though regional conflict has since been reported as testing the pace of that expansion.

Closer to home, the South Wales AI Growth Zone has been the subject of an estimated £10 billion of investment, with figures of up to £100 billion suggested across all UK AI Growth Zones.

Where reasons are given for choosing a particular location, they typically cite access to power (including renewable generation), available land, planning support and connectivity. This appraisal has not identified independent verification that these advantages outweigh the water and grid constraints discussed in Sections 4 and 5 below, and whether they make a location genuinely suitable, rather than merely available, should be treated as an open question rather than a settled one.[48,49]

---

[43] Tom's Hardware, 'Big Tech's AI Spending Plans Reach $725 Billion in 2026' (30 April 2026), reporting FT-compiled combined 2026 capital-expenditure guidance from Microsoft, Alphabet, Meta and Amazon, up from around $410 billion in 2025. https://www.tomshardware.com/tech-industry/big-tech/big-techs-ai-spending-plans-reach-725-billion

[44] CNBC, 'Alphabet (GOOGL) Q1 2026 Earnings Report' (29 April 2026), reporting 2026 capital expenditure guidance of up to approximately $190 billion. https://www.cnbc.com/2026/04/29/alphabet-googl-q1-2026-earnings.html

[45] CNBC, 'Microsoft (MSFT) Q3 FY2026 Earnings Report 2026' (29 April 2026), reporting 2026 capital expenditure guidance of approximately $190 billion. https://www.cnbc.com/2026/04/29/microsoft-msft-q3-earnings-report-2026.html

[46] MLQ News, 'Amazon Raises 2026 AI Capex to $220B, Says Capacity Won't Meet Demand Through 2027' (30 July 2026). https://mlq.ai/news/amazon-raises-2026-ai-capex-to-220b-says-capacity-wont-meet-demand-through-2027/

[47] Data Center Dynamics, 'OpenAI Announces Five More US Stargate Data Centers with Oracle and SoftBank' (24 September 2025), reporting committed Stargate sites of almost 7GW and over $400 billion of investment, against the original $500 billion, four-year headline announced in January 2025. https://www.datacenterdynamics.com/en/news/openai-announces-five-more-us-stargate-data-centers-with-oracle-and-softbank/

[48] Microsoft, 'Microsoft's $15.2 Billion USD Investment in the UAE' (3 November 2025); see also CNBC, 'Middle East War Testing Gulf's Ambitions to Become AI Hub' (24 May 2026), on the wider scale and fragility of Gulf-region AI infrastructure investment. https://blogs.microsoft.com/on-the-issues/2025/11/03/microsofts-15-2-billion-usd-investment-in-the-uae/

[49] Senedd Research (Welsh Parliament), 'Data Centres in Wales: How Will Wales Manage a Rapidly Growing Industry?' (2026), citing an estimated £10 billion in South Wales AI Growth

Whether investment of this scale is realistically deliverable is contested among analysts, and the material in this paragraph is commentary and opinion rather than established fact.

Sequoia Capital's David Cahn has argued, in an analysis first published in June 2024 and periodically updated, that a substantial and growing gap exists between AI infrastructure spending and the revenue AI companies currently generate, a concern echoed in mid-2026 reporting of rising anxiety in bond markets over debt-financed capital expenditure and increasingly circular investment arrangements between AI developers, cloud providers and chip manufacturers.

Other analysts have dismissed these concerns, pointing to continued revenue growth.

This appraisal takes no position on which view is correct; it notes only that credible, informed opinion is divided, and that a decision-maker relying on headline investment figures as evidence of deliverability would be relying on a contested assumption.[50]

A related and, so far as this appraisal has been able to establish, largely unexamined question is whether the headline investment figures already include the cost of the grid, transmission and water infrastructure needed to support the facilities they fund.

The evidence available suggests they generally do not.

National Grid's own material on connection reform notes sharply rising costs for transformers and overhead lines, and states an intention to protect existing and future customers from bearing the cost of building more network capacity than is needed, which implies that grid-reinforcement costs are substantially recovered through customer bills rather than from developers' own capital budgets.

If that is correct, the public and other electricity and water users, rather than the companies proposing the investment, may bear a material share of the infrastructure cost of accommodating it, potentially competing for funding with other infrastructure needs such as general grid decarbonisation or water-network renewal. This appraisal has not identified a published assessment that quantifies this effect, and the point is offered as a reasoned inference from the evidence available rather than an established fact.

Arising out of this, a potential question, which could be tabled by a Member of the Senedd to the Cabinet Minister for Enterprise, Connectivity and

---

Zone investment (with up to £100 billion suggested across all UK AI Growth Zones) and a UK grid connection queue of around 173 requests totalling over 100GW as of May 2026. https://research.senedd.wales/research-articles/data-centres-in-wales-how-will-wales-manage-a-rapidly-growing-industry/

[50] Sequoia Capital, David Cahn, 'AI's $600B Question' (20 June 2024, subsequently updated); see also CNBC, 'Bond Market Anxiety Is Growing Over AI Capex Budgets' (24 July 2026). These are analyst commentary and opinion, not independently verified fact, and are presented as such. https://www.sequoiacap.com/article/ais-600b-question/

Energy, or by a Member of Parliament to the Secretary of State for Energy Security and Net Zero, reads:

> *'What assessment has the [Welsh/UK] Government made of whether the capital expenditure announced by data-centre operators for facilities in [Wales/the UK] includes the cost of the grid, transmission and water infrastructure upgrades needed to support those facilities; and, if that cost is not included, what estimate has been made of who will bear it and whether it will compete with funding for other infrastructure priorities?'*

No answer to a question in these terms has been identified in Hansard, the Senedd Record or via WhatDoTheyKnow to date.

Data Retention and the Question of Necessity

A further, more basic question about the scale of data-centre demand deserves attention: how much of it is driven by an apparent assumption, shared across much of the industry and among individual users, that data passing through the internet should be retained indefinitely rather than deleted once it is no longer needed?

UK data protection law already addresses this in principle.

The storage limitation principle in Article 5(1)(e) UK GDPR requires personal data to be kept for no longer than necessary, though it leaves organisations to set and review their own retention periods rather than fixing them in law, and enforcement action specifically targeting excessive retention appears rare; a Finnish data protection authority fine of €856,000 in 2024 for failing to define a retention period at all illustrates the kind of enforcement this appraisal has not identified a UK equivalent for.[51,52]

Industry surveys have long suggested that a large proportion of stored data is never needed again. Veritas's widely cited 2016 'Global Databerg' report found that 85% of enterprise data surveyed was 'dark' (unclassified) or 'ROT' (redundant, obsolete or trivial); a similar 2018 survey found comparable results. This appraisal has not identified a large-scale study from 2023 to 2026 that refreshes those figures with current primary data,

[51] Information Commissioner's Office, 'Principle (e): Storage Limitation', UK GDPR guidance, requiring personal data to be kept 'for no longer than is necessary' but leaving retention periods to be set and reviewed by each organisation rather than fixing them in law. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/storage-limitation/

[52] European Data Protection Board, 'Finnish SA: Administrative Fine of EUR 856,000 for Failing to Define a Storage Period' (2024), an example of enforcement action against a failure to observe the storage-limitation principle; no directly comparable UK enforcement action penalising over-retention alone has been identified for the purposes of this appraisal. https://www.edpb.europa.eu/news/national-news/2024/finnish-sa-administrative-fine-eu-856000-failing-define-storage-period_pl

and they should be treated as an aging, vendor-commissioned claim rather than a current, independently verified fact.[53]

However, the evidence available suggests that the recent surge in data-centre capacity is driven predominantly by something other than (useful) long-term data retention.

The International Energy Agency's 2025 analysis of energy demand from AI found that data storage accounts for only around 5% of data-centre electricity consumption, while AI-optimised computing hardware, used for training and running AI models rather than for storing data, is projected to grow electricity use by roughly 30% a year and now drives close to half of global data-centre electricity growth.

On this evidence, characterising current data-centre expansion as primarily a consequence of 'saving everything' would not be accurate; the more significant driver, at least on current trends, is AI training and inference compute. This is an inference drawn by this appraisal from the IEA's figures, not a conclusion the IEA itself states, and I flag it as such.[54]

None of this makes data retention practice irrelevant to the wider question of necessity. A rule requiring organisations, and in particular the largest cloud and social-media operators, to demonstrate active use or a continuing lawful basis for data before it is retained beyond a defined period, rather than retaining it indefinitely by default, could plausibly reduce the storage component of data-centre demand, and would sit within the existing framework of UK data protection law rather than requiring wholly new legislation.

On the evidence available, however, such a rule should be understood as a modest and useful measure addressing one, currently secondary, driver of demand, rather than as an answer to the larger and faster-growing demand associated with AI compute addressed elsewhere in this appraisal.

---

[53] Veritas, 'Global Databerg Report' (15 March 2016), a widely cited industry survey finding that 85% of data stored by organisations surveyed was 'dark' (unclassified) or 'ROT' (redundant, obsolete or trivial); a comparable 2018 Veritas survey of UAE organisations found 81% unclassified. No large-scale study from 2023-2026 superseding these figures with fresh primary data has been identified, and the figures should be treated as an aging, vendor-commissioned survey claim rather than independently verified current fact. https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data

[54] International Energy Agency, 'Energy Demand from AI', in Energy and AI (2025), finding that storage systems account for only around 5% of data-centre electricity consumption, while AI-optimised 'accelerated servers' are projected to grow electricity use by roughly 30% a year, against approximately 9% a year for conventional servers, and now drive close to half of global data-centre electricity growth. This suggests that current data-centre capacity growth is driven predominantly by AI training and inference compute rather than by the long-term retention of data already collected, an inference drawn by this appraisal from the IEA's figures rather than a conclusion stated by the IEA itself. https://www.iea.org/reports/energy-and-ai/energy-demand-from-ai

4. Electricity Demand and Energy Infrastructure

Electricity demand represents one of the most significant issues associated with modern data centres.

Official statistics indicate that data centres consumed approximately 4.5 TWh of electricity in Great Britain during 2024, equivalent to around 2% of total grid consumption.[55]

The issue is not simply total demand but also geographical concentration. More than three quarters of national data-centre electricity consumption occurred in London and the South East.[56]

Concentrated growth may require:

- substation expansion;
- transmission upgrades;
- distribution-network reinforcement;
- additional generating capacity.[57]

Supporters regard such investment as part of the wider digital transformation of the economy.

Others question how increasingly energy-intensive infrastructure should be balanced against broader energy-transition and carbon-reduction objectives.[58,59]

[55] See n 7 above (DESNZ, Data Centre Electricity Consumption).
[56] See n 7 above (DESNZ, Data Centre Electricity Consumption).
[57] See n 7 above (DESNZ, Data Centre Electricity Consumption).
[58] See n 5 above (HoC Library, CBP-10315).
[59] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).

5. Water Use and Cooling Technologies

Water consumption has become an increasingly prominent issue internationally.

It is often suggested that many UK facilities consume comparatively modest quantities of water and that approximately half of surveyed English data centres employ waterless cooling technologies.[60]

At the same time, studies indicate that water use is concentrated among a relatively small number of very large facilities and that peak demand during hot weather may be more significant than annual averages.[61]

The principal cooling technologies include:

- air cooling;
- closed-loop chilled-water systems;
- evaporative cooling;
- direct liquid cooling;
- immersion cooling;
- hybrid systems.[62,63]

Each approach involves trade-offs between energy efficiency, water consumption, operational resilience and cost.

No single cooling technology can automatically be regarded as environmentally preferable in all circumstances.

The House of Commons Library briefing “Data centres: planning policy, sustainability, and resilience” records that environmental campaigners have criticised the lack of transparency regarding data-centre water consumption[64]. The figures that follow are sourced separately in the notes below.

A survey by techUK and the Environment Agency found that 51% of data centres in England used a waterless cooling system, 5% used water based cooling, and 44% used a hybrid system[65].

---

[60] See n 8 above (techUK, Water Use in England).
[61] See n 9 above (WRc, Data Centre Water Use Report).
[62] See n 8 above (techUK, Water Use in England).
[63] See n 9 above (WRc, Data Centre Water Use Report).
[64] House of Commons Library, 'Data centres: planning policy, sustainability and resilience', Research Briefing CBP-10315 (27 May 2026), which records that environmental campaigners have criticised the lack of transparency regarding data-centre water consumption. The figures quoted in the following paragraphs do not appear in this briefing and are sourced separately in the notes that follow. CBP-10315.pdf
[65] techUK, Understanding data centre water use in England, 18 August 2025. https://www.techuk.org/resource/techuk-report-understanding-data-centre-water-use-in-england.html The report's published summary confirms a voluntary survey of 73 facilities, the 51% figure for waterless cooling, and that 64% of responding sites used less than 10,000 cubic metres (10 million litres) a year; the other percentages quoted in the text have not been re-

Of the sites who provided information about their water consumption:

- 33% used less than 1 million litres of water per year.
- 31% used between 1 million and 10 million litres per year.
- 14% used between 10 million and 100 million litres per year.
- 4% used over 100 million litres per year.

However, this survey did not collect any other information about the data centres it covered (such as type, age, and size).

The report also acknowledges that the survey was conducted on a voluntary and anonymous basis, meaning that the results may be skewed by who chose to respond.

Even this questionable data should cause questions to be asked. The so-called waterless cooling systems seem to use a considerable amount of water. Note that it is admitted that the data is not full and there is no data to tell the public how high the figures actually go. This data stops at “over 100 million litres per year” with no admission as to how high the numbers go.

Kept from the public: the EU's reporting rules for data centres

The European Union has gone further than the United Kingdom in one respect.

Since 2024, operators of data centres with an installed IT power demand of at least 500 kW must report their energy use, water use, use of renewable energy and reuse of waste heat to a European database. But the Commission regulation that set the scheme up requires the Commission and Member States to 'keep confidential all information and key performance indicators for individual data centres'; only aggregated national figures are published.[66]

In April 2026 an investigation published by Investigate Europe, with Corporate Europe Observatory and AlgorithmWatch, reported that Microsoft and the industry body DigitalEurope, whose members include Amazon, Google and Meta, had each proposed identical wording making all information about individual data centres confidential, and that the Commission had copied it into the regulation almost word for word.[67] Ten legal scholars told Investigate Europe that the clause could conflict with the Aarhus Convention on public access to environmental information, and

checked against the full report.

[66] Commission Delegated Regulation (EU) 2024/1364 of 14 March 2024 on the first phase of the establishment of a common Union rating scheme for data centres, Article 5(5); see also n 68 below for the text of the clause. https://eur-lex.europa.eu/eli/reg_del/2024/1364/oj/eng

[67] AlgorithmWatch and Corporate Europe Observatory, 'Copy, paste, govern: Microsoft ghostwrote EU policy that keeps data centers' energy use secret' (17 April 2026), research published by Investigate Europe. https://algorithmwatch.org/en/copy-paste-govern-microsoft-ghostwrote-eu-policy/; https://corporateeurope.org/en/2026/04/copy-paste-govern

ClientEarth raised concerns; Microsoft said that it supports greater transparency around data centres.[68]

On 21 September 2026 the Commission adopted a further regulation creating a public sustainability label for each data centre, expected to be displayed from 2027, showing grades for energy and water use, the energy mix and readiness to reuse waste heat. It amends the confidentiality clause 'to allow for the publication of the labels', but it still requires the Commission and Member States to treat as confidential 'all information and key performance indicators for individual data centres', with the exception of the information that forms part of the label. The grades will therefore be public, while the figures behind them for each site will not. The new regulation is subject to scrutiny by the European Parliament and the Council before it takes effect.[69]

In the author's view, the case for keeping these figures confidential is weak, for four reasons.

- First, they describe the use of resources that are shared and, in a drought or a congested grid, scarce: drinking water, grid capacity and the generation behind it, the costs of which fall partly on the public.
- Secondly, planning authorities, regulators and communities cannot judge the cumulative effect of several data centres on one catchment or one part of the grid without figures for each site.
- Thirdly, annual totals of energy and water use for a building reveal little that a competitor could use; that is the author's assessment rather than an established finding.
- Fourthly, the EU's own decision to publish grades concedes that the public has a legitimate interest in this information.

In the United Kingdom, a public body holding such information would face the Environmental Information Regulations 2004, which require 'a presumption in favour of disclosure' and provide that information on emissions cannot be withheld on grounds of commercial confidentiality at all.[70]

---

[68] DataCenterDynamics, 'Data center lobby secured EU provision to keep environmental impact data confidential - report' (18 April 2026). https://www.datacenterdynamics.com/en/news/data-center-lobby-secured-eu-provision-to-keep-environmental-impact-data-confidential-report/

[69] European Commission, 'Making data centres energy efficient thanks to a new EU rating system' (21 September 2026); Commission Delegated Regulation establishing a common Union rating scheme for data centres, C(2026) 3472 final, Explanatory Memorandum, Articles 3 and 5(3). https://commission.europa.eu/news-and-media/news/making-data-centres-energy-efficient-thanks-new-eu-rating-system-2026-09-21_en; https://energy.ec.europa.eu/document/download/b073ba9b-82a8-45cb-b8ba-78dad149e941_en?filename=C_2026_3472_1_EN_ACT_part1_v9.pdf

[70] Environmental Information Regulations 2004 (SI 2004/3391), regulation 12(2) (presumption in favour of disclosure) and regulation 12(9) (information on emissions not to be withheld under the exceptions in regulation 12(5)(d) to (g), which include commercial confidentiality). https://www.legislation.gov.uk/uksi/2004/3391/regulation/12

Whether energy and water figures count as information on emissions has not, so far as this appraisal can establish, been tested; the emissions from standby generators plainly would.

The more immediate point is that the United Kingdom has no requirement at all for individual data centres to report their energy or water use, so even the EU's imperfect scheme is ahead of it.

The author intends to put the following question in writing to Kanishka Narayan MP, as Minister for Artificial Intelligence, asking that it also be put to the Secretary of State for Energy Security and Net Zero:

> *'Will the Government introduce mandatory reporting of energy and water use by individual data centres in the United Kingdom, published site by site, and will it ensure that such figures are not withheld from the public on grounds of commercial confidentiality?'*

A request via WhatDoTheyKnow to the Department for Energy Security and Net Zero for any assessment it holds of mandatory data-centre reporting, and of the EU scheme, might follow the reply.

And to the Welsh Government Cabinet Secretary responsible for climate change and the environment a request could be made:

> *'Will the Welsh Government require operators of data centres in Wales, through planning conditions or otherwise, to publish each year their energy use and their water use, including peak-month water use, for each site; and what information on the energy and water use of individual data centres in Wales does the Welsh Government or Natural Resources Wales currently hold?'*

A request via WhatDoTheyKnow to the Welsh Government and to Natural Resources Wales for the information they hold could be made at the same time.

In answer to a Parliamentary Question the Minister in June 2025 (the specific question and its reference have not yet been located in the UK Parliament written questions database, and needs to be confirmed before this passage is relied on publicly) confirmed that:

> *Data centre water consumption varies considerably based on their size and cooling method. There is currently no requirement for data centres to report on their water consumption, so an accurate assessment of their impact on water supplies to consumers and agriculture is difficult. We are working with data centres and their trade associations to understand their impact and identify opportunities to improve reporting and water efficiencies in their design.*

Tim Squirrel, head of strategy at campaign group Foxglove, criticised the techUK report's "methodological flaws"[71].

Environmental groups have also criticised industry-reported figures for ignoring indirect water consumption, such as water used to generate electricity to power data centres[72].

The Guardian has estimated that if indirect water consumption is included, the first two data centre halls at the site in Blyth, Northumberland could consume 124 million litres of water per year, rather than the 2.3 million litres claimed by the developer[73]. It appears possible that developers and, possibly, Government want us to focus on parts of their environmental impacts but avoid joining the various dots involved in an Environmental Impact Assessment to avoid the sort of arguments that need to be (should be) addressed.

The water sector has expressed concern that while annual water consumption may be relatively low, water demand from data centres peaks on the hottest days, when the water network is already "stretched"[74]. We do not know whether this is based on the figures the industry admits to rather than the real world scenario.

WaterUK estimates that UK data centres have an average peak water demand of 14 million litres per day - a figure for peak demand, such as on hot summer days, rather than for everyday use; Water UK's corresponding estimate of average daily demand is around 6.6 million litres[75]. Thames Water has said it is engaging with data centre operators to mitigate this, including by encouraging the use of on-site water storage systems and installing flow restrictors to prevent data centres from drawing more water

[71] Computer Weekly, TechUK report on datacentre water usage habits criticised, 12 September 2025. https://www.computerweekly.com/news/366630713/TechUK-report-on-datacentre-water-usage-habits-criticised

[72] Global Action Plan, Not a drop to drink: how Britain's data centre surge threatens water security (PDF), April 2026. https://www.globalactionplan.org.uk/insights/publications/not-a-drop-to-drinkhow-britains-data-centre-surge-threatens-water-security

[73] Guardian, UK's largest proposed datacentre 'understating planned water use', 19 December 2025. The web address of the original Guardian article has not been located for this appraisal. The same comparison, that the site could use around 50 times more water than the developer claims once indirect use is included, was reported by edie: https://www.edie.net/uks-largest-planned-data-centre-could-use-50-times-more-water-than-developer-claims/ (behind a paywall, and not independently read for this appraisal).

[74] Thames Water, EIR-23-24-469, 13 December 2023; Water Research Centre, Water efficient data centres, February 2026, p3. The Water Research Centre report is at https://www.wrcgroup.com/uploads/Water%20Efficient/Water%20Efficient%20Data%20Centres.pdf; it confirms that water companies' main concern is demand on peak days, which is likely to coincide with high domestic demand, but the word 'stretched' has not been located in it, and the Thames Water response has not been re-checked.

[75] Times, Surge in data centres set to push water bills even higher, 10 May 2026. Full Fact has since explained that the 14 million litres a day figure is Water UK's estimate of average peak demand, such as on hot summer days, and that average daily use is around 6.6 million litres: https://fullfact.org/environment/times-water-data-centres/

than agreed[76]. However, the public needs to understand what data is being relied on.

Local interest in water supplies

Whichever cooling technology a data centre uses, water is central to its operation:

- directly, through evaporative or liquid cooling systems, and
- indirectly, through the water consumed in generating the electricity the facility draws from the grid.

That reliance does not disappear where a facility advertises low or 'net positive' operational water use, since the wider water system - the pipework, treatment works and reservoirs a facility and its surrounding area share - still needs to be resilient enough to meet peak demand, including from users other than the data centre itself.

South Wales, in common with much of England, has experienced drought conditions before and is expected to do so again; meteorologists and farming organisations have separately warned of increasingly unpredictable rainfall as the climate changes.

Against that background, it is a fair question what would happen to a water-cooled data centre, and to the businesses and public services that come to depend on it, during a prolonged water shortage - and specifically, on what basis, if any, such a facility would be required to reduce or cease its own water use before household or agricultural supplies were affected.

In response to an enquiry made of a UK Government minister about the water demands of data centres in a drought scenario, the assurance given was that data centres do not use as much water as is sometimes suggested and that, in any event, industrial users including data centres would be required to reduce or stop using water before households were affected.

This appraisal has not been able to identify any published UK/Welsh Government assessment, specific to data centres, that sets out the evidential or legal basis for that assurance, including how it would operate in practice, who would decide when it applied, and how compliance would be monitored.

The assurance given has never been put in writing to me and subsequent correspondence remains unanswered – for now.

Three further points arise, which are the author's own.

- First, even a 'closed-loop' cooling system is not sealed for ever: pipework leaks, systems are drained for maintenance, and the loss

[76] Thames Water, EIR-23-24-469, 13 December 2023; see also Data Center Dynamics, 'Thames Water May Restrict London Data Centers' Water Use' (26 July 2023): https://www.datacenterdynamics.com/en/news/thames-water-may-restrict-london-data-centers-water-use/

has to be made good, so a closed loop still draws water, and its demand is least predictable when something goes wrong.

- Secondly, where water is taken from the public supply and treated with chemicals to protect the cooling system, it cannot simply be returned to that supply for households or farming; what happens to that water, and where it is discharged, is a matter that an environmental impact assessment ought to address.[77]
- Thirdly, it is hard to believe that investors would commit sums on this scale without some assurance about water in a drought. If such assurances have been given, it should be known by whom, on what terms, and how they sit with the duties in the Well-being of Future Generations (Wales) Act 2015.

That gap matters because the UK Government has designated data infrastructure as part of the nation's Critical National Infrastructure, as noted above. Critical National Infrastructure status is capable, in principle, of supporting a case for prioritising a facility's utility supplies over other users during a shortage, in the way long established for infrastructure such as hospitals and emergency services.

Whether that status has been, or would be, relied upon in that way for data centres - and, if so, on what public and transparent basis - does not appear to be addressed in published planning or drought-management policy.

The underlying concern is not hypothetical. Research published in April 2026 found that 84% of the water-intensive data-centre developments proposed in the UK are in areas that are already water-stressed or are projected to be so by 2040, with London and the South East particularly affected; Slough alone was found to host at least 32 operational data centres in an area officially classified as ‘seriously water stressed’.[78]

Research by Global Action Plan has estimated that data centres could drive almost 30% of all new water demand in the Thames Water region, around 270 million litres a day; Thames Water itself indicated in 2023 that it was considering measures such as flow restrictors and premium peak-demand

[77] On the chemistry and treatment of cooling-system discharge water, see S T Ahmad and others, 'Recovery and treatment of cooling tower blowdown water: challenges, recent advancement, and future perspectives', Journal of Environmental Chemical Engineering (2025). The three points in the text are the author's own. https://doi.org/10.1016/j.jece.2025.115399

[78] Global Action Plan research reported in Water Magazine, '84% of Proposed UK Data Centres to be Built in Water-Stressed Areas' (27 April 2026). https://www.watermagazine.co.uk/2026/04/27/84-of-proposed-uk-data-centres-to-be-built-in-water-stressed-areas/ The original research is Global Action Plan, 'Report reveals majority of new data centres planned for water stressed areas' (7 April 2026), which puts the figure at 84% of water-intensive data-centre developments proposed for areas that are already water-stressed or projected to be so by 2040: https://www.globalactionplan.org.uk/insights/news/report-reveals-majority-of-new-data-centres-planned-for-water-stressed-areas

charges specifically for data-centre customers, alongside encouraging on-site water reuse and recycling.[79]

No equivalent public assessment of water-stress classification specific to proposed data-centre sites in Wales has been identified in the course of this appraisal - itself a gap worth noting. The National Infrastructure Commission for Wales has since recorded that new water users 'are likely to start to increase in Wales in this period, particularly data centres and hydrogen power', that pressures on supply will be 'particularly acute in the southern areas of Wales where the water resource zones are more stressed', and that the water requirements of sectors such as agriculture fall outside the normal scope of water resource management plans. Southern Wales is where most of the data-centre capacity proposed in Wales is concentrated (see Section 15 below).[80]

North Wales provides the clearest published illustration so far of how variable a single site's water demand may be.

The Environmental Statement for the proposed Menai Data Centre at Griffiths Crossing, near Caernarfon (Gwynedd Council application C25/0740/20/EIA, Gwelyfenai Ltd), is reported to give a maximum water demand of 'approximately 11,949,120 litres per day' against an expected normal use of 'approximately 700,000 litres per day', with a proposed electricity connection of 450 MW.

Dŵr Cymru Welsh Water is reported to have raised concerns about 'the capacity of local sewerage infrastructure and the information available on cooling technology and water requirements', and the cooling technology, and whether it would use PFAS-containing fluids, had not been confirmed.

The site lies beside the Menai Strait, part of a marine Special Area of Conservation.[81] These figures are taken from the North Wales Rivers Trust's and the Menai Strait Partnership Forum's accounts of the Environmental Statement; the author has not yet examined the Statement or Dŵr Cymru's consultation response directly.[82]

Two observations follow, both the author's own arithmetic and inference rather than findings of any source.

---

[79] Data Center Dynamics, 'Thames Water May Restrict London Data Centers' Water Use' (26 July 2023). https://www.datacenterdynamics.com/en/news/thames-water-may-restrict-london-data-centers-water-use/ The estimate that data centres could drive almost 30% of all new water demand in the Thames Water region, around 270 million litres a day, is from Global Action Plan, 'Report reveals majority of new data centres planned for water stressed areas' (7 April 2026): https://www.globalactionplan.org.uk/insights/news/report-reveals-majority-of-new-data-centres-planned-for-water-stressed-areas

[80] National Infrastructure Commission for Wales, 'Wales Infrastructure Assessment 2026: Water' (March 2026). https://nationalinfrastructurecommission.wales/water26/

[81] North Wales Rivers Trust, 'The Menai Data Centre: At What Cost?' (September 2026), summarising the Environmental Statement for Gwynedd Council application C25/0740/20/EIA. https://northwalesriverstrust.org/news/the-menai-data-centre-at-what-cost

[82] Menai Strait Partnership Forum, 'Menai Data Centre - At What Cost?' (18 September 2026). https://www.menaiforum.org/2026/09/menai-data-centre-at-what-cost/

- First, the reported maximum is about seventeen times the expected normal figure, and it is the maximum, not the normal, that a water supplier must be able to meet, typically on the hottest days when other demand also peaks.
- Secondly, the reported maximum for this one site is of the same order as Water UK's estimate of about 14 million litres a day for the average peak demand of all UK data centres together, discussed above.

If the reported figures are accurate, a single large proposal in a part of Wales outside the more stressed southern water resource zones could on its own add peak demand comparable to the whole existing sector's, which underlines why the basis of the maximum figure, the cooling technology chosen and the arrangements that would apply in a drought should be established before a decision is taken.

The author intends to put the following question in writing to Gwynedd Council, as local planning authority (Head of Planning), copied to Dŵr Cymru Welsh Water:

'For application C25/0740/20/EIA,

1. on what assumptions does the Environmental Statement rest for the maximum water demand of about 11.95 million litres a day and the expected normal demand of about 700,000 litres a day;
2. in what conditions, and for how many days a year, is demand expected to approach the maximum;
3. what cooling technology is proposed and will it use PFAS-containing fluids; and
4. has Dŵr Cymru confirmed that the maximum can be supplied, and the resulting wastewater treated, without affecting other customers or the Menai Strait Special Area of Conservation?'

A request from a local resident might stand more chance of a response.

No answers to the questions in these terms have been identified. The author will consider a request via WhatDoTheyKnow to Gwynedd Council for the consultation responses of Dŵr Cymru and Natural Resources Wales if adequate responses are not on the public file.

None of this is put forward as a case against data-centre development in principle, nor as a finding that assurance given to this appraisal is wrong. It is put forward because water security - whether, on what terms, and at whose ultimate cost a reliable supply can be guaranteed to a large, new industrial user - is properly a matter for the planning and environmental impact process to test before consent is considered/granted, rather than a matter to be resolved informally, or only once a shortage has occurred.

It also engages the duties in the Well-being of Future Generations (Wales) Act 2015,[83] discussed further below. Whether those duties are given substantive rather than procedural effect in decisions of this kind is something this appraisal, from published material alone, is not able to verify.

[83] Welsh Government, Well-being of Future Generations (Wales) Act 2015: The Essentials. https://www.gov.wales/well-being-future-generations-act-essentials-html

6. Carbon Emissions and Climate Change

Assessment of climate impacts should extend beyond operational electricity use.

A comprehensive appraisal should consider:

- Direct emissions, including:
  - backup generators,
  - fuel combustion and
  - refrigerant leakage.
- Indirect emissions including:
  - imported electricity and
  - cooling-system energy requirements.
- Embodied emissions including emissions associated with:
  - steel,
  - concrete,
  - batteries,
  - servers,
  - network infrastructure and
  - construction activity.

Whole-life assessment has become increasingly important because embodied carbon may represent a significant proportion of total lifecycle impacts.

Climate resilience also requires attention.

Facilities expected to operate for decades must function under future conditions that may involve increased temperatures, more frequent heatwaves, droughts and severe weather events.[84,85,86]

As with water consumption, the picture on carbon emissions is clouded by significant gaps in what is measured and reported. Despite data centres being identified as one of the fastest-growing sources of UK electricity demand, they were not separately disaggregated in the Government's official projections underpinning the Seventh Carbon Budget, the statutory emissions pathway to 2040.[87]

In February 2026, the Secretary of State for Energy Security and Net Zero, Ed Miliband, acknowledged in correspondence with the Environmental Audit Committee that future electricity demand from data centres ‘remains inherently uncertain’, prompting the Committee to launch a dedicated

[84] See n 1 above (DSIT, WMS HCWS89).
[85] See n 5 above (HoC Library, CBP-10315).
[86] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).
[87] House of Commons Environmental Audit Committee, written evidence: data centres and the Seventh Carbon Budget (2026), noting the omission of disaggregated data-centre demand from the Climate Change Committee's carbon budget projections. https://committees.parliament.uk/writtenevidence/151599/html/

inquiry into the sector's sustainability, including whether existing carbon-budgeting and planning policy adequately account for AI-driven demand growth.[88]

Rhetorically the author might ask, why is this “inherently uncertain” if there is transparency of information from the Industry?

This uncertainty is not confined to the Climate Change Committee's modelling. In answer to a written parliamentary question in April 2026, the Government confirmed that it does not disaggregate specific estimates for data-centre electricity demand within its wider projections, relying instead on the Clean Power 2030 Action Plan and the Capacity Market to balance overall supply and demand.[89]

In other words, the same absence of dedicated, mandatory reporting identified above in relation to water consumption applies with equal force to carbon. Government policy is, on its own admission, being made without a clear picture of the demand it is trying to manage.

Backup and standby generation compounds the difficulty. Many large facilities maintain extensive diesel or gas generator capacity to protect against grid outages. As with water storage and abstraction, there is no comprehensive, published national record of how often these generators run, for how long, or what they emit in aggregate, whether during routine testing or at times of grid stress when their use - and their emissions - would be highest.[90]

Embodied emissions from construction, servers and network hardware raise a parallel concern. Whole-life carbon assessments depend on manufacturers' and developers' own disclosures, which are neither independently verified nor consistently reported across the sector.

As with water, this is not necessarily evidence that data-centre carbon impacts are being concealed.

It is evidence that neither government nor the public currently has the data needed to state with confidence what those impacts are, now or as AI-driven demand grows.

Until reporting is put on a mandatory and independently verifiable footing, planning authorities, the Climate Change Committee and Parliament itself

---

[88] House of Commons Environmental Audit Committee, MPs to Examine Data Centres' Climate Impact as Miliband Says Future Demand 'Inherently Uncertain' (February 2026). https://committees.parliament.uk/committee/62/environmental-audit-committee/news/212132/mps-to-examine-data-centres-climate-impact-as-miliband-says-future-demand-inherently-uncertain/

[89] UK Parliament, Written Question 127433, Dame Chi Onwurah to the Secretary of State for Energy Security and Net Zero, answered by Michael Shanks MP (24 April 2026). https://questions-statements.parliament.uk/written-questions/detail/2026-04-15/127433

[90] Browne Jacobson, NPPF 2026 Amendments: Data Centres and On-Site Energy Generation (2026). https://www.brownejacobson.com/insights/nppf-2026-amendments-browne-jacobson-response/data-centres-and-on-site-energy-generation

are being asked to take reassurances on trust rather than on evidence - precisely the situation in which, as discussed in Section 17 below, a precautionary approach is warranted.

7. Energy-from-Waste and Incinerator-Related Power

Some developers have explored direct relationships between data centres and Energy-from-Waste (EfW) facilities.

Such arrangements may provide reliable electricity supplies and potentially reduce transmission losses.[91]

However, EfW remains controversial within environmental policy. Debate continues regarding carbon emissions, air quality and compatibility with wider recycling objectives.[92]

The appropriate question is therefore not whether EfW is inherently beneficial or harmful, but whether environmental impacts have been transparently assessed and compared with realistic alternatives.

Waste heat: a resource the planning system has not yet asked about

Almost all of the electricity used by a data centre's computing equipment ends up as heat, which its cooling systems then reject to the air or to water.

That is a matter of basic physics rather than a finding of any source cited here, and it means that a facility drawing 150 MW is, in effect, a continuous source of low-grade heat of broadly that order.

Whether that heat is wasted or put to use is decided largely by where a facility is sited and how it is laid out - in other words, at the planning stage, before the design is fixed.

The point is not new. For combustion and energy-from-waste power plants, Natural Resources Wales has since 2014 expected applicants to show that plants are 'CHP-Ready', able to supply heat in future, observing that 'to be commercially viable for CHP, new plants should ideally be sited close to potential heat loads'.[93]

Experience in Cardiff shows what retrofitting involves: the Cardiff Heat Network, which takes heat from Viridor's Trident Park energy recovery facility, was costed at £26.5 million, with a £6 million UK Government grant and an £8.6 million Welsh Government loan, and delivered its first heat in November 2025.[94] The Welsh Government's Heat Strategy for Wales (2024)

[91] House of Commons Library, Incineration of Waste in England, Research Briefing CBP-10229 (April 2025). https://commonslibrary.parliament.uk/research-briefings/cbp-10229/
[92] Ibid.
[93] Natural Resources Wales, 'CHP-Ready Guidance for Combustion and Energy from Waste Power Plants' (version 2, September 2014). https://naturalresourceswales.gov.uk/media/2100/chp-ready-guidance-for-combustion-and-energy-from-waste-power-plants.pdf
[94] Resource, '£15m funding approved for Cardiff district heat network' (14 August 2020); Business News Wales, 'Cardiff Heat Network delivers first low carbon heat' (November 2025). https://www.resourcemedia.eco/article/15m-funding-approved-cardiff-district-heat-network;

cites the Cardiff network as an example of using waste heat; this appraisal has found no reference in it to data centres.[95]

The legal framework in England and Wales is narrower than is sometimes assumed.

Schedule 24 to the Environmental Permitting (England and Wales) Regulations 2016, which carries forward requirements of the Energy Efficiency Directive, requires an application for an environmental permit for certain installations with a net rated thermal input exceeding 20 MW to include a cost-benefit analysis of 'utilising the waste heat to satisfy economically justified demand, including through cogeneration' and of 'the connection of that installation to a district heating and cooling network'.[96]

Data centres come within environmental permitting mainly because of their standby generators: the Environment Agency, for example, permits large sites as combustion installations, with emergency operation limited by condition to 500 hours a year.[97] Standby and peak-load plant of that kind is largely outside the cost-benefit requirement, and this appraisal has found no example of the analysis being required for the heat produced by the computing equipment itself, which is not in itself a permitted activity.

The position may be different where a site will depend, possibly for years, on continuously running on-site generation while it waits for a grid connection, as the Cardiff East proposal described below may. Whether Schedule 24 then applies, and to what, is a question this appraisal would put to Natural Resources Wales rather than answer. It is the author's own reading of the Regulations, not an established interpretation.

Elsewhere the obligation is direct.

Under the recast EU Energy Efficiency Directive, data centres with a total rated energy input above 1 MW must use their waste heat, or other waste-heat recovery applications, unless they can show that this is not technically or economically feasible.[98]

Germany's Energy Efficiency Act goes further, requiring new data centres to

https://businessnewswales.com/cardiff-heat-network-delivers-first-low-carbon-heat/

[95] Welsh Government, 'Heat Strategy for Wales' (July 2024). https://www.gov.wales/sites/default/files/publications/2024-07/heat-strategy-wales.pdf

[96] Environmental Permitting (England and Wales) Regulations 2016 (SI 2016/1154), Schedule 24, 'Efficiency in heating and cooling energy: Energy Efficiency Directive', paragraphs 1 to 3. https://www.legislation.gov.uk/uksi/2016/1154/schedule/24

[97] Environment Agency, decision document for a bespoke permit for standby electricity generating combustion plant at a data centre site operated by Amazon Data Services UK Limited (29 January 2026). https://assets.publishing.service.gov.uk/media/69846ade468d351e1406b4b8/Application_Bespoke_A001_Decision_Document_-_29012026.pdf

[98] Directive (EU) 2023/1791 on energy efficiency (recast), Article 26(6); for a summary, see Covington & Burling, 'The EU's Energy Efficiency Directive and its impact on datacenters' (2025). https://eur-lex.europa.eu/eli/dir/2023/1791/oj/eng; https://www.cov.com/-/media/files/corporate/publications/2025/04/the-eus-energy-efficiency-directive-and-its-impact-on-datacenters.pdf

plan for at least 15% reused waste heat from July 2026, rising to 20% from July 2028.[99]

In England, the Government confirmed in January 2026 that, under heat network zoning, a zone coordination body will be able as a backstop to require a heat source within or around a zone 'to provide heat where connection is viable'. Heat network zoning applies to England only.[100]

This appraisal has not identified any equivalent requirement in Wales, or any reference to data-centre waste heat in Welsh or UK planning policy on data centres.

Food security, glasshouses and water reuse

The United Kingdom produces about 62% of the food it consumes, 53% of its fresh vegetables and only 16% of its fresh fruit, and the Government's own food security report records that several major supplying countries, including Spain, face increasing drought and heat stress.[101]

The Welsh Government said in December 2024 that 'there is a need now to cultivate more fruit and vegetables in Wales', including 'protected cultivation crops in glasshouses and polytunnels', and that more horticulture could strengthen 'system resilience and food security'.[102]

Low-grade heat is what glasshouses need through the colder months. Proposals to pair the two already exist in the United Kingdom: the Humber Tech Park scheme in North Lincolnshire, a proposed 386 MW data-centre campus, included a greenhouse of some 300,000 square feet for growing tomatoes with captured waste heat.[103]

This appraisal has not established whether that scheme has been consented or built. In the author's view - an inference, not a finding of any source - co-locating large data centres with commercial-scale glasshouses or district heat networks is one of the few ways in which a data centre's

---

[99] Kristin Weiß, 'From EU Framework to National Action: How Germany Regulates Data Center Energy Use', Sabin Center for Climate Change Law, Columbia Law School (24 October 2025), on section 11 of the Energy Efficiency Act (EnEfG). https://blogs.law.columbia.edu/climatechange/2025/10/24/from-eu-framework-to-national-action-how-germany-regulates-data-center-energy-use/

[100] Department for Energy Security and Net Zero, 'Heat network zoning consultation 2023: summary of government response' (21 January 2026). https://www.gov.uk/government/consultations/proposals-for-heat-network-zoning-2023/outcome/heat-network-zoning-consultation-2023-summary-of-government-response

[101] Department for Environment, Food and Rural Affairs, 'United Kingdom Food Security Report 2024: Theme 2: UK Food Supply Sources' (11 December 2024). https://www.gov.uk/government/statistics/united-kingdom-food-security-report-2024/united-kingdom-food-security-report-2024-theme-2-uk-food-supply-sources

[102] Welsh Government, 'Written Statement: Horticulture policy development in Wales' (18 December 2024). https://www.gov.wales/written-statement-horticulture-policy-development-wales

[103] DatacenterDynamics, report on the Humber Tech Park planning application, North Lincolnshire (18 May 2024). https://www.datacenterdynamics.com/en/news/humber-tech-park-lincolnshire-uk-district-heating/

physical footprint could make a direct and lasting contribution to the community and the food system around it, and whether it has been considered should be asked of every large proposal before its site and layout are fixed.

Water offers a parallel opportunity, to be approached with more caution. Facilities using evaporative cooling discharge 'blowdown' water in which minerals and treatment chemicals become concentrated; a 2025 review concluded that such water 'can be effectively recycled', but only with specialised treatment.[104]

Reusing treated discharges or harvested rainwater for irrigation could reduce competition with farming for water in a drought, but would first need to be shown to be safe, including in respect of any PFAS used on site (see Section 8). Air-cooled designs, such as the Cardiff East proposal below, use little process water but must dispose of more heat to the air, which strengthens the case for asking what is done with that heat. The figures can also change after an application is made: later documents for Cardiff East describe a closed-loop system, with the final choice still open, and seek an allowance of up to 300 cubic metres of water a day.[105]

Case study: Cardiff East Park and Ride

The proposal for a data centre at the Cardiff East Park and Ride site at Pentwyn, on land owned by Cardiff Council, illustrates these points.[106]

A report to the Council's Cabinet in May 2021 records that the land was marketed for a logistics centre with ancillary retail, keeping the Park and Ride; that the preferred developer, Curtis Hall, is to deliver a new bridge and road link into Llanrumney in lieu of a land receipt; and that completion of the sale is subject to planning.[107] The Council is therefore both the planning authority and a landowner whose sale depends on permission being granted. The Wales EIA Regulations require it to perform its duties objectively and so as to avoid a conflict of interest.[108]

---

[104] S T Ahmad and others, 'Recovery and treatment of cooling tower blowdown water: challenges, recent advancement, and future perspectives', Journal of Environmental Chemical Engineering (2025). https://doi.org/10.1016/j.jece.2025.115399

[105] Water Usage Datasheet for application 26/00109/HYB, published on the Cardiff Council planning register on 6 October 2026. https://www.cardiffidoxcloud.wales/publicaccess/files/0B1B9164A37A106ADEC41E1D472E8976/pdf/26_00109_HYB-WATER_USAGE_DATASHEET-6465333.pdf

[106] Nation.Cymru, 'Data centre plans put on hold as ministers intervene' (4 September 2026), Local Democracy Reporting Service. https://nation.cymru/news/data-centre-plans-put-on-hold-as-ministers-intervene/

[107] Cardiff Council, Cabinet, 20 May 2021, agenda item 9, 'Llanrumney Regeneration Scheme – Statutory Public Consultation and Land Disposal Update', paragraphs 6, 7 and 24 to 27 (public reports pack, pages 359 to 363). https://cardiff.moderngov.co.uk/documents/g4316/Public%20reports%20pack%2020th-May-2021%2014.00%20Cabinet.pdf?T=10&LLL=0

[108] Town and Country Planning (Environmental Impact Assessment) (Wales) Regulations 2017, regulation 58. https://www.legislation.gov.uk/wsi/2017/567/regulation/58

The hybrid application (reference 26/00109/HYB), submitted in January 2026, seeks permission for data-centre buildings with a capacity of 150 MW and an 'ancillary energy centre (maximum 47 MW capacity)', described as a temporary energy centre needed because 'a connection to the grid may not be possible until after the data centres have been constructed and brought into use'. As first submitted, cooling was to be by air handling units using external air. The applicant's Planning Statement relies on the Welsh Government's AI Plan for Wales and on UK Government support for data centres, but contains no discussion of using the development's waste heat or of a heat network.[109]

The Planning Statement also records that formal scoping for the Environmental Statement 'has not been repeated, given the similarities between the schemes', and that the Environmental Statement prepared for an earlier permission for commercial units on the site has been 'suitably updated'; it says this approach was agreed with the Council.

Noise is treated as a non-EIA matter on the basis that this was 'agreed with the Council during the initial EIA scoping', although the scheme now includes back-up generators and a possible temporary energy centre.[110]

The scoping opinion on which the assessment therefore rests (reference SC/21/00018/MJR, issued in 2022) was given for a 'commercial development'. It agreed that 'Energy and Sustainability' could be scoped out, while adding that the assessment 'should also consider if a local heat network is feasible'. It asked for greenhouse gas emissions to be scoped in; and it reminded the applicant that an environmental statement must estimate emissions including 'heat'.[111] The screening opinion (reference SC/21/00006/MJR) is recorded only by reference in these documents, and the two documents give different dates for it; the author has not yet located it on the public file.

In the author's view - an inference, and not a finding of any public body - a 150 MW data centre with on-site generation is a materially different development from the commercial units for which the scope of assessment

---

[109] Iceni Projects for Curtis Hall Limited, 'Planning Statement: Cardiff Park and Ride East, Pentwyn' (January 2026), paragraphs 2.6, 2.12, 4.22-4.24, 5.6-5.8, 6.36-6.44 and 6.85, application 26/00109/HYB, Cardiff Council planning register. https://www.cardiffidoxcloud.wales/publicaccess/applicationDetails.do?keyVal=T8YL3PECJ8T00&activeTab=summary

[110] Iceni Projects for Curtis Hall Limited, 'Planning Statement: Cardiff Park and Ride East, Pentwyn' (January 2026), paragraphs 2.6, 2.12, 4.22-4.24, 5.6-5.8, 6.36-6.44 and 6.85, application 26/00109/HYB, Cardiff Council planning register. https://www.cardiffidoxcloud.wales/publicaccess/applicationDetails.do?keyVal=T8YL3PECJ8T00&activeTab=summary

[111] Cardiff Council, Screening and Scoping Opinion, reference SC/21/00018/MJR, Cardiff East Park and Ride (2022), reproduced as Environmental Statement Volume II, Appendix 1.2, application 26/00109/HYB. https://www.cardiffidoxcloud.wales/publicaccess/applicationDetails.do?keyVal=T8YL3PECJ8T00&activeTab=documents

was settled in 2022, particularly as regards energy demand, heat, generator noise and emissions, and the case for fresh scoping was strong.

Whether the Environmental Statement deals adequately with those matters is now also a question for Welsh Ministers, who in September 2026 issued a holding direction preventing the Council from granting permission while they decide whether to determine the application themselves,[112] and potentially for Natural Resources Wales if on-site generation requires an environmental permit.

Since the application was made, later documents on the register have changed its description. The energy centre, put at 47 MW in the application, had by October 2026 become seven gas turbines on 'duty/standby' feeding a steam turbine, with controls to keep output below 49.9 MW, just under the 50 MW point at which the Welsh Ministers, not the Council, decide. The cooling system has changed, and the air quality conclusion on generator testing has moved from 'significant' to not significant. The public has been invited to comment four times, each time on part of the material.[113] A fuller account, with sources, is in the case study on the website for this paper, and the author and Max Wallis have made representations to the Council.[114]

The author might put the following questions in writing to Cardiff Council, as local planning authority (Head of Planning) (although they may be better sent by a local resident):

'In relation to application 26/00109/HYB:

1. why was a new scoping opinion not required, when the 2022 scoping opinion (SC/21/00018/MJR) was given for commercial units rather than a 150 MW data centre with a 47 MW energy centre;
2. does the Environmental Statement quantify the waste heat the development would produce and assess the feasibility of using it, as the 2022 opinion asked in respect of a local heat network;
3. will the Council publish screening opinion SC/21/00006/MJR; and
4. do the Heads of Terms agreed with Curtis Hall for the sale of the site allow a data centre and gas-fired energy centre, when the land was marketed for a logistics centre, and what arrangements has the Council made to keep its interest as landowner separate from its role as planning authority?'

[112] Nation.Cymru, 'Data centre plans put on hold as ministers intervene' (4 September 2026), Local Democracy Reporting Service. https://nation.cymru/news/data-centre-plans-put-on-hold-as-ministers-intervene/

[113] Cardiff Council planning register, application 26/00109/HYB, documents tab (including the Technical Note (Air Quality), combined reports, 6 October 2026, at https://www.cardiffidoxcloud.wales/publicaccess/files/54C572792D4179F901419D580EE3D9FC/pdf/26_00109_HYB-TECHNICAL_NOTE__AIR_QUALITY__-_COMBINED_REPORTS-6465338.pdf): https://www.cardiffidoxcloud.wales/publicaccess/applicationDetails.do?activeTab=documents&keyVal=T8YL3PECJ8T00

[114] Questions Before Concrete, 'Case study: Cardiff East', https://environment.cymru/case-cardiff-east.html; representations by Dennis Clarke and Max Wallis: https://environment.cymru/papers/cardiff-east-data-centre-representations-clarke-wallis.pdf

A request via WhatDoTheyKnow for the correspondence in which it was agreed that scoping need not be repeated, for the screening opinion, and for the Heads of Terms (which the Council may withhold as commercially confidential), could follow.

To Natural Resources Wales:

'Will the temporary energy centre of up to 47 MW and the standby generators proposed at Cardiff East require an environmental permit; if so,

1. will the application have to include the cost-benefit analysis required by Schedule 24 to the Environmental Permitting (England and Wales) Regulations 2016;
2. does Natural Resources Wales consider that the analysis can extend to the heat produced by the data-centre equipment; and
3. has it advised, or will it advise, Welsh Ministers on these matters?'

A request via WhatDoTheyKnow for any pre-application or permitting correspondence on the site could be a natural follow-up.

To the Welsh Government Cabinet Secretary responsible for planning:

'Will the Welsh Government

1. require proposals for large data centres to show how their waste heat will be used, or why it cannot be, as it expects of combustion and energy-from-waste plant;
2. will it consider co-location of data centres with heat networks or commercial glasshouses as part of its horticulture and food-security policy; and
3. will it take these matters into account in deciding whether to determine the Cardiff East application itself?'

A request via WhatDoTheyKnow for any advice to Ministers on data-centre waste heat could follow once a reply is received.

And to the Vale of Glamorgan Council, as local planning authority, and the Welsh Government, as landowner at Bro Tathan: 'For any further data-centre development at Bro Tathan,

1. will any screening or scoping opinion require an assessment of the quantity of waste heat produced and the feasibility of using it, including for heat networks or horticulture, and
2. of the reuse of any process water?'

A request via WhatDoTheyKnow for any screening or scoping opinions already issued for data-centre development at Bro Tathan would establish the current position.

8. Local Environmental Effects

Large facilities may generate:

- continuous mechanical noise;
- low-frequency vibration;
- construction traffic;
- visual impacts;
- air-quality effects from backup generation;
- waste heat.[115,116]

Because many facilities operate continuously, night-time impacts require particular attention.

Research is also beginning to explore whether concentrated clusters may contribute to localised heat-island effects. Further evidence will be required before firm conclusions can be drawn.[117]

Chemicals of concern in construction and operation, including PFAS 'forever chemicals'

A further concern raised in relation to data-centre development is the use of hazardous chemicals, and in particular per- and polyfluoroalkyl substances (PFAS), often called 'forever chemicals' because their carbon-fluorine bonds resist natural breakdown and can persist in soil, water and living tissue for decades.

Three distinct uses arise in this sector, and this appraisal treats them separately because the evidence, and the appropriate response, differs for each:

1. dielectric cooling fluids used inside some immersion-cooling systems;
2. clean-agent fire-suppression gases used to protect server halls without water damage; and
3. PFAS used far upstream, in the manufacture of the semiconductors that data centres run.[118]

On cooling fluids, the picture is contested.

3M, formerly the leading manufacturer of two-phase immersion-cooling fluids (marketed as Novec and Fluorinert, both PFAS), announced in December 2022 its intention to exit all PFAS manufacturing by the end of

[115] See n 5 above (HoC Library, CBP-10315).
[116] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).
[117] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).
[118] 3M, '3M to Exit PFAS Manufacturing by the End of 2025' (20 December 2022), announcing the phase-out of all per- and polyfluoroalkyl substance (PFAS) manufacturing, including the Novec and Fluorinert product lines used as two-phase immersion-cooling fluids in some data centres. https://news.3m.com/2022-12-20-3M-to-Exit-PFAS-Manufacturing-by-the-End-of-2025

2025, and single-phase immersion-cooling fluids, typically mineral, synthetic or plant-derived oils, are not PFAS.

However, a September 2026 survey by the Swedish chemicals watchdog ChemSec, reported by the Guardian, found that nine of the world's ten biggest PFAS manufacturers - including Chemours, Daikin, Arkema, AGC, Dongyue, Gujarat Fluorochemicals, HaloPolymer, Orbia and Syensqo - now plan to increase production, citing demand from AI data-centre cooling and semiconductor manufacture specifically. Only Archroma and BASF (the latter by 2028) were reported as moving away from PFAS. [119]

On this evidence, 3M's departure from the market appears to be the exception rather than the industry direction.

This appraisal has not identified a published, site-by-site account of PFAS-based cooling fluid use, continuing or discontinued, across the UK data-centre estate, nor any UK-specific data on whether developers here are among those now placing orders with the expanding manufacturers identified in the ChemSec survey; both are accordingly genuine, and so far as this appraisal can establish, unanswered questions.[120]

On fire suppression, the position is less reassuring than it may first appear. Data-centre fire codes generally specify clean-agent gases such as FM-200 (HFC-227ea) or Novec 1230 (FK-5-1-12) rather than water-based sprinklers or aqueous film-forming foam (AFFF), precisely because they are non-conductive and leave no residue on electronic equipment.

Under the broad structural definition of PFAS now used by the OECD, and increasingly by UK and EU regulators, these clean agents are themselves PFAS, distinct from the AFFF more commonly associated with contamination at airports and military sites.

This appraisal has not identified confirmed evidence that AFFF is in routine use inside operational data-centre halls specifically, and treats that particular claim as contested; the clean-agent alternatives that are specified, however, remain PFAS on the definition now in general regulatory

[119] Damien Gayle, "'Tidal wave' of Pfas being launched to satisfy AI industry, campaigners warn", the Guardian (14 September 2026), reporting a survey by the Swedish chemicals watchdog ChemSec of the world's ten biggest PFAS manufacturers, which found that nine plan to increase production, several citing demand from AI data-centre cooling and semiconductor manufacture specifically; only Archroma and BASF (by 2028) were reported as moving away from PFAS. This appraisal has not independently located ChemSec's own underlying report or survey methodology, and relies here on the Guardian's reporting of it. https://www.theguardian.com/environment/2026/sep/14/pfas-firms-tidal-wave-forever-chemicals-ai-industry-demand-datacentres

[120] Submer, 'PFAS Contamination: A Call to Action for the Datacenter Industry' (2026), describing PFAS as the chemical basis of two-phase immersion-cooling fluids and cautioning that, following bans on some PFAS formulations, manufacturers have in some cases reformulated products that remain PFAS under the broad definition while being marketed as 'green' alternatives. https://submer.com/blog/pfas-contamination-a-call-to-action-for-the-datacenter-industry/

use.[121,122]

On semiconductor manufacture, PFAS use is well documented in photolithography and etching processes, but this occurs almost entirely outside the United Kingdom, principally in Taiwan, South Korea and the United States, and is a matter for the chip supply chain rather than for a UK or Welsh data-centre site itself.

This appraisal notes it as relevant context for the sector's overall PFAS footprint - and for the working conditions of people employed in chip manufacture, a workforce quite separate from the data-centre construction and operational staff considered later in this section - rather than treating it as a local environmental effect of any specific UK development.[123]

On quantities, this appraisal has not identified any published figure - litres of cooling fluid, kilograms of fire-suppression agent, or any other measure - specific to UK or Welsh data centres, whether for an individual facility or in aggregate.

In the absence of that data, no reliable extrapolation of the quantities of PFAS-related chemicals likely to be needed to supply the possible future extent of data-centre development in England and Wales can responsibly be offered; any such figure would be speculation dressed as analysis.

What can be said is only that the underlying drivers - more facilities, larger facilities, and a continuing (if declining) reliance on PFAS-containing fire-suppression and, to a lesser and diminishing extent, cooling technologies - point toward greater rather than lesser aggregate use while that reliance continues, a directional inference rather than a quantified one.

On environmental release and water contamination, PFAS's defining property - persistence - is also what makes any release into soil or water difficult to remedy once it occurs.

---

[121] Organisation for Economic Co-operation and Development, 'Reconciling Terminology of the Universe of Per- and Polyfluoroalkyl Substances' (2021), setting out the broad structural definition of PFAS now generally used in UK and EU regulatory practice. https://www.oecd.org/en/publications/reconciling-terminology-of-the-universe-of-per-and-polyfluoroalkyl-substances_e458e796-en.html

[122] NFPA 2001, Standard on Clean Agent Fire Extinguishing Systems, is the industry standard governing clean-agent gases such as FM-200 (HFC-227ea) and Novec 1230 (FK-5-1-12), chosen for data-centre use because they are non-conductive and leave no residue on electronic equipment; under the broad OECD definition of PFAS referred to above, these clean agents themselves fall within the PFAS family, distinct from the aqueous film-forming foam (AFFF) more commonly associated with contamination at airports and military sites. https://www.nfpa.org/product/nfpa-2001-standard/p2001code/nfpa-2001-standard-on-clean-agent-fire-extinguishing-systems-2015/200115

[123] ZVEI (German Electro and Digital Industry Association), 'PFAS and Semiconductors' factsheet, describing PFAS use in semiconductor photolithography (as photoresist surfactants and photoacid generators) and in plasma etching (fluorine-based gases used to structure silicon, dielectric and metal layers), and noting that no drop-in substitute currently exists for most such uses. https://www.zvei.org/fileadmin/user_upload/Themen/Nachhaltigkeit_Umwelt/PFAS/2-ZVEI-Factsheet-_PFAS_and_Semiconductors_-final.pdf

PFAS compounds bioaccumulate in the food chain and are associated in the scientific and regulatory literature with a range of health effects at sufficient exposure, which is why drinking-water limits exist at all.

UK regulatory protection for PFAS in drinking water is currently uneven: the Drinking Water Inspectorate's January 2025 guidance for England and Wales recommends a cumulative limit of 100 nanograms per litre across 48 named substances, but this is guidance rather than a statutory duty, whereas Scotland has applied a statutory limit for 20 named PFAS substances since January 2023.

The EU's revised Drinking Water Directive imposes a statutory total-PFAS limit from January 2026, a protection now available to EU citizens but not, in equivalent statutory form, to those in England and Wales.

Once PFAS enters a water source, contamination can render that source unfit for drinking, agricultural or other uses for a period measured in decades rather than months, which is why prevention rather than remediation is generally treated as the only realistic policy response.[124,125]

This appraisal has not identified any confirmed instance of environmental contamination traced to a UK data centre specifically, whether affecting the surrounding environment, nearby residents, or a water supply.

The best-documented example of PFAS harm connected to this broader industrial family - contamination near Chemours's Fayetteville Works manufacturing facility in North Carolina - is a chemical-manufacturing case, not a data-centre case, and should not be read as evidence of an established data-centre-specific risk. US commentators have nonetheless begun explicitly connecting the AI data-centre boom to PFAS use, including reporting in September 2026 and a campaign-group report published in July 2026; this appraisal has not identified equivalent UK-specific reporting or research making the same connection for data centres in England or Wales.

The absence of a confirmed UK incident is not, on its own, evidence that no risk exists, particularly given the limited reporting requirements on data-centre chemical use noted throughout this appraisal; it is evidence only that

[124] Chemistry World, 'Water regulator applies stricter PFAS limits to drinking water in England and Wales' (2024), reporting the Drinking Water Inspectorate's guidance, expected to take effect from January 2025, introducing a cumulative limit of 100 nanograms per litre across 48 individual PFAS substances for England and Wales - guidance rather than a statutory duty, in contrast to Scotland's statutory limit for 20 named PFAS substances since January 2023. https://www.chemistryworld.com/news/water-regulator-applies-stricter-pfas-limits-to-drinking-water-in-england-and-wales/4020476.article

[125] Directive (EU) 2020/2184 on the quality of water intended for human consumption (the revised Drinking Water Directive) sets a total-PFAS limit of 0.5 micrograms per litre, which took effect across EU member states from 12 January 2026; the UK, no longer bound by EU directives following its withdrawal from the European Union, instead relies on the non-statutory Drinking Water Inspectorate guidance for England and Wales referred to above. https://environment.ec.europa.eu/news/new-eu-rules-limit-pfas-drinking-water-2026-01-12_en

no such incident has yet come to light.[126,127]

On the people most directly affected - those working in data-centre construction and operation, rather than those working in semiconductor manufacture considered above - occupational exposure to fire-suppression and cooling-fluid chemicals during installation, maintenance, testing and any accidental discharge is the pathway most directly within a UK employer's control, and the one for which UK health and safety law already provides a regulatory route, through the control-of-substances-hazardous-to-health framework.

This appraisal has not identified any published assessment specific to data-centre construction or maintenance workers' PFAS exposure, whether from the Health and Safety Executive or from industry, and treats that as a further, specific gap rather than an assumption that no risk exists.

On decommissioning, UK PFAS regulation is only now beginning to develop and is not yet focused on data centres.

The Department for Environment, Food and Rural Affairs published the UK's first dedicated PFAS strategy - the 'PFAS Plan' - on 3 February 2026, updated 17 August 2026, adopting the broad OECD definition of PFAS and committing to a 2026 consultation on a statutory drinking-water limit and to reforming UK REACH so that chemical protections can be applied in a way that is 'more aligned with our closest trading partners, especially the EU, by December 2028'; commentary from the chemicals-policy organisation ChemTrust has described the Plan as prioritising further research over immediate regulatory action, in contrast with the EU's more advanced timetable.

Separately, the Health and Safety Executive has been consulting on a possible UK REACH restriction on 'PFAS in Firefighting Foams' specifically, in two stages: an initial consultation on the risk-assessment case opened in August 2025, and a further consultation on the socio-economic case opened in July 2026 and closed on 7 September 2026, with HSE's opinion on the risk assessment already given ahead of that second-stage consultation and a government decision still awaited.

---

[126] US Environmental Protection Agency, National Primary Drinking Water Regulation for PFAS (final rule, April 2024), setting enforceable limits of 4.0 parts per trillion for PFOA and PFOS, with public water systems given until 2029 to comply; the EPA's own 'Proposed PFAS Rescission Rule' and a related proposal to extend the PFOA/PFOS compliance deadline, both published in 2026, illustrate that this regulatory position remains contested and unsettled even in the jurisdiction that has gone furthest toward statutory limits, and are cited here as international regulatory context rather than as a statement of UK law. https://www.epa.gov/sdwa/and-polyfluoroalkyl-substances-pfas

[127] Department for Environment, Food and Rural Affairs, 'PFAS Plan' (published 3 February 2026, updated 17 August 2026), the UK Government's first dedicated PFAS strategy, adopting the broad OECD definition of PFAS and committing to a 2026 consultation on introducing a statutory drinking-water limit and to aligning with EU REACH restrictions 'by December 2028'. https://www.gov.uk/government/publications/pfas-plan

This is a consultation confined to firefighting foam rather than to the clean-agent suppression gases more commonly used inside data centres, so its eventual relevance to data-centre decommissioning, if any, remains uncertain.[128]

This appraisal has not identified any published UK or Welsh guidance addressing what happens to PFAS-containing fire-suppression systems, or any residual PFAS-containing cooling fluid, when a data centre is decommissioned, refurbished or demolished.

Natural Resources Wales's own State of Natural Resources Report 2025 identifies PFAS as a contaminant of concern in Welsh waters generally, but neither that report nor any other published Natural Resources Wales or Welsh Government material identified for this appraisal addresses PFAS specifically in the context of data centres or their decommissioning; this appraisal treats that as a genuine and citable gap in Welsh environmental regulatory coverage, while noting that Natural Resources Wales's statutory remit and resources are matters beyond this appraisal's scope to assess.

As an illustrative, and deliberately non-comparable, order-of-magnitude reference point for the scale of liability that PFAS-specific remediation can generate once identified across a cluster of sites, the US Government Accountability Office reported in 2025 that the US Department of Defense's own estimate of its future PFAS-specific investigation and cleanup costs had risen to more than $9.3 billion for fiscal year 2025 and beyond, more than tripling since 2022; this figure is cited purely to illustrate how quickly such liability can grow once quantified, not as a claim that any comparable liability has arisen, or should be expected, from UK or Welsh data-centre

[128] Health and Safety Executive, UK REACH consultations on 'PFAS in Firefighting Foam': an initial consultation on the risk-assessment case opened in August 2025, and a further consultation on the socio-economic case opened 9 July 2026 and closed 7 September 2026, with HSE's opinion on the risk assessment already published ahead of that second-stage consultation; a government decision on any restriction is still awaited. https://consultations.hse.gov.uk/crd-reach/uk-reach-restriction-on-pfas-in-firefighting-foam/

development.[129,130,131,132]

A more concrete illustration, and one now adjudicated rather than merely estimated, comes from New Jersey.

On 8 August 2026 a US federal court approved settlements totalling approximately $2.5 billion, payable over 25 years, between the State of New Jersey and DuPont-related entities (around $2.075 billion in total, combining an $875 million payment into funds for natural-resource restoration and drinking-water-system remediation with a further $1.2 billion in additional remediation commitments) and 3M (a further $400-450 million), arising from decades of PFAS manufacturing contamination in the state. [133]

---

[129] US Government Accountability Office, GAO-25-107401, 'Persistent Chemicals: DOD Needs to Provide Congress More Information on Costs Associated with Addressing PFAS' (reissued with revisions, February 2025), reporting that the Department of Defense's own estimate of its future PFAS-specific investigation and cleanup costs had risen to more than $9.3 billion for fiscal year 2025 and beyond, more than tripling since 2022; cited here purely as an illustrative order-of-magnitude comparator for the scale and volatility of PFAS-specific liability once quantified, and not as a claim that any equivalent liability has arisen, or is expected to arise, from UK or Welsh data-centre development, for which this appraisal has identified no comparable costed assessment. https://www.gao.gov/products/gao-25-107401

[130] Natural Resources Wales, State of Natural Resources Report 2025, Pollution chapter, which identifies 'PFAS, veterinary medicines and other pharmaceuticals' as contaminants of concern in Welsh waters generally but does not address data centres as a source, and does not otherwise engage with PFAS in the context of data-centre construction, operation or decommissioning; this appraisal has not identified any other published Natural Resources Wales guidance, assessment or monitoring programme that does so, which it treats as a genuine and citable gap in Welsh environmental regulatory coverage rather than as an oversight necessarily attributable to Natural Resources Wales itself, whose statutory remit and resources are matters beyond this appraisal's scope. https://naturalresources.wales/evidence-and-data/research-and-reports/state-of-natural-resources-report-2025/pollution/?lang=en

[131] North Carolina Department of Environmental Quality, GenX Investigation: Groundwater, documenting PFAS/GenX contamination of industrial and residential groundwater wells near Chemours's Fayetteville Works manufacturing facility, first identified in 2017 and the subject of a February 2019 Consent Order; this is a well-documented example of PFAS harm linked to chemical manufacturing, not to a data centre, and this appraisal has not identified any confirmed instance, in the United Kingdom or elsewhere, of environmental contamination traced to a data centre specifically. Chemours agreed a further $450 million settlement covering Fayetteville Works and three other US sites in June 2026, illustrating that liability from PFAS-manufacturing contamination remains an active and growing matter even for a case dating to 2017. https://www.deq.nc.gov/news/key-issues/genx-investigation/groundwater

[132] Reporting has begun explicitly connecting the AI data-centre boom to PFAS use, including Jessica Corbett, 'Research Warns of Surge in Cancer-Causing Forever Chemicals From AI Data Center Build-Out', Common Dreams (14 September 2026), and Food & Water Watch, 'Toxic Mixture: Data Centers Turn to PFAS For Cooling' (July 2026). This appraisal has not identified equivalent UK-specific reporting or research making the same connection for data centres in England or Wales, which this appraisal treats as an emerging area of scrutiny elsewhere rather than as a topic yet addressed by UK press, regulators or campaigners in relation to domestic sites. https://www.commondreams.org/news/data-centers-and-pfas

[133] New Jersey Office of the Attorney General, 'Federal Court Approves Historic PFAS Settlements Valued at Approximately $2.5 Billion' (press release, 8 August 2026); see also the joint New Jersey Department of Environmental Protection news release of the same date, and reporting in the Philadelphia Inquirer, 'Federal court approves settlements that will pay New Jersey $2.5 billion for PFAS contamination' (8 August 2026), from which the breakdown of payments between DuPont-related entities and 3M given in the text is drawn.

This settlement concerns chemical-manufacturing sites, not a data centre, and this appraisal does not suggest that a comparable liability has arisen, or is likely to arise, from UK or Welsh data-centre development; but it is a materially firmer data point than the Department of Defense estimate above, since it reflects a sum a court has actually approved rather than an agency's own internal projection, and it involves two of the same companies - DuPont and 3M - whose PFAS products feature elsewhere in this section.

Whether the scale of liability that can attach to PFAS manufacturing, once identified, has any read-across to the manufacturers now expanding PFAS production for the AI and data-centre market identified above is, on the evidence available to this appraisal, an open question rather than one this appraisal is in a position to answer.

A question naturally arising from PFAS's multi-decade persistence is whether this issue has serious repercussions for the seven-generations principle underpinning the Well-being of Future Generations (Wales) Act 2015.

This appraisal has not identified any published material in which the Welsh Government, the Senedd or the Future Generations Commissioner for Wales has connected forever-chemical contamination to the seven-generations or long-term thinking duties in that Act.

The connection drawn here is accordingly this appraisal's own inference, offered because the reasoning appears to follow naturally from the Act's own stated purpose and from PFAS's documented persistence, and not because any existing Welsh policy document makes the link.

On its face, a chemical class capable of remaining in the environment for longer than a human generation, let alone seven, is difficult to reconcile with a duty to safeguard the ability of future generations to meet their own needs; but this appraisal is not aware of that reasoning having been tested, applied or even considered in any published Welsh Government, Senedd or Future Generations Commissioner material to date, and flags the point as an original inference requiring independent verification rather than as an established finding.[134]

A suggested written question, which could be tabled by a Member of the Senedd to the Cabinet Secretary with responsibility for climate change and rural affairs, or put by correspondence to Natural Resources Wales, reads:

'What assessment has the Welsh Government or Natural Resources Wales made of

https://www.njoag.gov/federal-court-approves-historic-pfas-settlements-valued-at-approximately-2-5-billion/

[134] See n 83 above (Welsh Government, Well-being of Future Generations (Wales) Act 2015: The Essentials). The connection drawn in the text between the persistence of PFAS and the duties in that Act is this appraisal's own inference; no published Welsh Government, Senedd or Future Generations Commissioner source making it has been identified.

1. the use of PFAS ('forever chemicals') in the fire-suppression and cooling systems of data centres operating or proposed in Wales, including the quantities used, the risk of environmental release, and
2. what guidance, if any, exists on the safe decommissioning of such systems; and
3. does that assessment have regard to the duties in the Well-being of Future Generations (Wales) Act 2015?'

No answer to a question in these terms has been identified in the Senedd Record or via WhatDoTheyKnow to date.

A request to Natural Resources Wales via WhatDoTheyKnow, seeking any risk assessment, monitoring data or decommissioning guidance specific to PFAS use at data-centre sites in Wales, would be a further and more direct available route, and has not, so far as this appraisal is aware, yet been made. The author believes that NRW's involvement in regulating forever chemicals might be on the low side, at best.

A further written question, which could be tabled by a Member of Parliament to the Secretary of State for Environment, Food and Rural Affairs, reads:

'In light of ChemSec's September 2026 survey finding that nine of the world's ten largest PFAS manufacturers plan to increase production to meet demand from artificial intelligence data centres,

1. what assessment has the Department made of whether the evidence base underpinning the PFAS Plan published on 3 February 2026 and updated on 17 August 2026 accounted for this trend; and
2. does the Department intend to revisit the Plan's timetable for aligning with EU REACH restrictions, currently set at December 2028, in light of it?'

No answer to a question in these terms has been identified in Hansard or via WhatDoTheyKnow to date. A freedom of information request to the Department for Environment, Food and Rural Affairs via WhatDoTheyKnow, seeking any internal assessment of the ChemSec survey or of AI-driven PFAS demand more generally, could be a further and more direct available route, and has not, so far as this appraisal is aware, yet been made.

9. Digital Sovereignty, Jurisdiction and Public Trust

Data-centre discussions increasingly extend beyond environmental impacts and into questions of governance.

Modern cloud infrastructures commonly involve information being processed, stored and replicated across multiple locations. Ownership, operational control, legal responsibility and physical location may not always coincide.[135,136]

This complexity has encouraged growing interest in concepts such as:

- data residency;
- digital sovereignty;
- sovereign cloud services;
- operational control.

Physical storage within a particular jurisdiction does not automatically resolve all questions of governance and accountability.

Whether existing arrangements are sufficient is ultimately a question of public policy rather than purely technical analysis.

[135] Information Commissioner's Office, Adequacy Regulations (updated July 2026). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/adequacy-regulations/

[136] Information Commissioner's Office, UK Extension to the EU-US Data Privacy Framework (updated July 2026). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/adequacy-regulations/how-does-the-uk-extension-to-the-eu-us-data-privacy-framework-work/

10. International Data Transfers and Jurisdictional Complexity

Modern digital infrastructures routinely rely upon backup, replication and disaster-recovery arrangements extending across multiple sites.

Such arrangements typically improve resilience and service continuity.[137,138]

At the same time, they may raise questions including:

- To what extent should backup locations be disclosed?
- Should different categories of information be treated differently?
- Is data residency equivalent to data sovereignty?
- How should resilience benefits be balanced against increasing jurisdictional complexity?

These questions do not imply flaws in existing arrangements. They reflect the reality of increasingly sophisticated and geographically distributed digital infrastructures.

The author admits to being unable to resolve apparent issues that appear to arise as between the GDPR and the way in which the internet seems to operate.

A search can be carried out with a result that the person searching will be supplied with information that might be gathered from any jurisdiction connected to the WWW where such information is available to a search engine. In the same way, a search from another jurisdiction can result in information being scraped from eg a website, social media etc where information may have been uploaded. Information and data can, in this way, find its way from the UK to any other jurisdiction without worrying about the limitations imposed on the transfer of information out of the jurisdiction.

This appraisal does not, cannot, explain how GDPR fits into this.

[137] See n 135 above (ICO, Adequacy Regulations).
[138] See n 136 above (ICO, UK Extension to the EU-US DPF).

11. The CLOUD Act and International Governance

Legal commentators have identified continuing debate regarding the interaction between cross-border disclosure obligations under the United States CLOUD Act and European concepts of data sovereignty.

At the same time, UK organisations remain subject to UK GDPR and to applicable transfer mechanisms recognised by the Information Commissioner's Office.[139,140]

The existence of these debates should not be interpreted as evidence of unlawful disclosures.

Rather, they demonstrate the complexity that can arise when infrastructure, information flows and legal authority operate across national boundaries.

We are looking at the issues that could arise in the near and distant future where the UK might be assuming a world order that did exist and hopes it will persist. At the same time huge power is to be vested in a few super rich individuals who are not elected representatives and whose ambitions might not align with the need to maintain what we presently consider to be a rule of law.

[139] See n 135 above (ICO, Adequacy Regulations).
[140] See n 136 above (ICO, UK Extension to the EU-US DPF).

12. Public-Sector Data and National Sovereignty

Particular attention is often directed towards public-sector information.

Examples include:

- healthcare records;
- justice-system information;
- policing data;
- taxation records;
- critical-infrastructure information.

Questions raised in policy discussions include:

- Should certain categories of information remain under domestic legal control?
- Is physical storage within the UK sufficient?
- Should backup arrangements be subject to additional scrutiny?
- How should governments balance innovation, research, efficiency and sovereignty?

These questions concern governance and public confidence rather than simple technical compliance.

Questions of sovereignty should also be distinguished from questions of privacy. Information may be processed lawfully while debate continues regarding appropriate legal and operational control.

Recent experience: Palantir in the UK public sector, and the United States 'DOGE' episode

Two recent episodes show that the questions above are not abstract. Neither concerns a data centre in Wales, and neither is evidence that data held in the United Kingdom has been misused. They are included because they show how questions of control, as distinct from questions of physical location, arise in practice.

The first concerns Palantir Technologies, a US-headquartered data-analytics company. In November 2023 NHS England awarded Palantir a contract worth £330 million over seven years for its Federated Data Platform.[141]

NHS England states that each NHS trust and integrated care board remains the data controller for its own instance, that patient data is 'retained within

[141] The Stack, 'NHS signs Palantir up under £330 million NHS data contract' (21 November 2023). https://thestack.technology/nhs-signs-palantir-up-under-330-million-nhs-data-contract

the UK region', and that Palantir 'cannot commercialise or market NHS data, even on an anonymised basis'.[142]

Palantir has since entered a strategic partnership with the Ministry of Defence, announced in September 2025 alongside up to £1.5 billion of Palantir investment in the United Kingdom and defence opportunities 'worth up to £750 million over the next five years',[143] and was selected in 2026 for a £9 million Home Office contract to replace the national firearms licensing system.[144] More than a quarter of the 43 police forces in England and Wales have been reported to be involved in Palantir pilots, although none of the forces named is Welsh.[145]

In June 2026 the House of Commons Science, Innovation and Technology Committee concluded: 'Of the small number of technology providers that the UK public sector relies upon, Palantir concerns us most.'

It described Palantir's increasing presence across the public sector as 'an unacceptable point of weakness', while stating that this view was 'not ideologically motivated or driven by concerns about the quality of their products', and it recommended that the Government commit to exercising the February 2027 break clause in the Federated Data Platform contract.

More generally, the Committee found that 'the UK's reliance on a small number of US-based providers for digital infrastructure and public service delivery is a strategic and economic vulnerability', and recorded concerns that under the CLOUD Act US-headquartered companies 'could in principle be compelled to provide the US Government with access to UK customers' data held in their UK data centres' (see Section 11 above).[146] Separately, the platform's whole-life cost has been revised upwards to £1.1 billion and its

---

[142] NHS England, 'NHS Federated Data Platform: frequently asked questions'. https://www.england.nhs.uk/digitaltechnology/nhs-federated-data-platform/fdp-faqs/

[143] Ministry of Defence, 'New strategic partnership to unlock billions and boost military AI and innovation' (press release, 18 September 2025). https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation

[144] PublicTechnology, 'Palantir picked for new £9m national gun database as MPs join opposition to US firm's public sector deals' (3 June 2026). https://www.publictechnology.net/2026/06/03/business-and-industry/palantir-picked-for-new-9m-national-gun-database-as-mps-join-opposition-to-us-firms-public-sector-deals/

[145] Computing, 'More than a quarter of England and Wales police forces now involved in Palantir pilots' (7 September 2026), reporting research by the Financial Times; the forces named are all English, together with the Metropolitan Police. https://www.computing.co.uk/news/2026/government/more-than-a-quarter-of-england-and-wales-police-forces-now-involved-in-palantir-pilots

[146] House of Commons Science, Innovation and Technology Committee, 'Rewiring the state: Delivering digital government' (report, 3 June 2026), conclusions and recommendations on Palantir, technological sovereignty and the CLOUD Act; see also the Committee's press notice of the same date. https://publications.parliament.uk/pa/cm5902/cmselect/cmsctech/61/report.html; https://committees.parliament.uk/committee/135/science-innovation-and-technology-committee/news/214048/mps-warn-that-palantirs-increasing-presence-in-the-uk-public-sector-is-an-unacceptable-point-of-weakness/

forecast benefits reduced to £808 million; Palantir has said the programme 'remains on track from a project-delivery perspective'.[147]

The Federated Data Platform is an NHS England programme. This appraisal has found no published information on whether NHS Wales bodies or the Welsh Government use Palantir software, and has not located a published Government response to the Committee's report.

The second episode concerns the United States 'Department of Government Efficiency' (DOGE) in 2025.

In June 2025 the US Supreme Court allowed DOGE team members access to Social Security Administration records while litigation continued.[148] In August 2025 the Administration's chief data officer, Charles Borges, made a whistleblower disclosure to the Office of Special Counsel and to Congress alleging that DOGE personnel had created 'a live copy of the country's Social Security information in a cloud environment that circumvents oversight', covering more than 300 million Americans. The Administration responded that the data was held in a secure environment and that it was 'not aware of any compromise'.[149]

In January 2026, however, a Justice Department court filing acknowledged that DOGE staff had shared data through links on a third-party server, Cloudflare, and that the Administration did not know what data had been shared or whether it remained there.[150]

A further, anonymous, allegation in March 2026, that a former DOGE engineer had retained Social Security databases on a thumb drive, is under review by the Administration's Inspector General and has been denied by all those named.[151]

---

[147] Computing, 'NHS Palantir platform's business case under pressure as costs rise and benefits fall' (10 August 2026). https://www.computing.co.uk/news/2026/government/nhs-palantir-platform-s-business-case-under-scrutiny-as-costs-rise-and-benefits-fall

[148] Supreme Court of the United States, Social Security Administration v American Federation of State, County and Municipal Employees, No 24A1063, order of 6 June 2025 staying the preliminary injunction pending appeal. https://www.supremecourt.gov/opinions/24pdf/24a1063_6j37.pdf

[149] Government Accountability Project, 'Whistleblower warns of possible risks to Americans' Social Security information' (press release, 26 August 2025); for the Administration's response, see Government Accountability Project, 'Whistleblower claims DOGE compromised Social Security data of hundreds of millions of Americans' (reproducing The Independent). https://whistleblower.org/press-release/whistleblower-warns-of-possible-risks-to-americans-social-security-information/; https://whistleblower.org/in-the-news/the-independent-whistleblower-claims-doge-compromised-social-security-data-of-hundreds-of-millions-of-americans/

[150] Government Executive, 'DOGE officials face Hatch Act referrals for work with org aiming to "overturn election results"' (January 2026), reporting the Justice Department's court filing of January 2026. https://www.govexec.com/management/2026/01/doge-officials-face-hatch-act-referrals-work-org-aiming-overturn-election-results/410825

[151] NPR, 'The government is investigating new claims that DOGE misused Social Security data' (12 March 2026), as published by OPB. https://www.opb.org/article/2026/03/12/new-investigations-look-at-doge-and-social-security-data/

Palantir was reported in April 2025 to be involved in a separate DOGE effort to build a single 'mega API' for accessing Internal Revenue Service records.[152]

This appraisal has found no evidence that Palantir was involved in the Social Security incidents described above, and none are inferred.

What follows is this appraisal's own inference, not a finding of any of the sources cited.

The lesson of these episodes is not that one company or one administration is uniquely untrustworthy. It is that legal and contractual safeguards for data are only as strong as the willingness and ability of those who operate the systems to observe them, and that the political direction of the state in which a provider is headquartered can change quickly.

In the United States case, the data was held by the state's own agencies in its own jurisdiction, and physical location gave no protection against people with wide administrative access acting outside normal controls.

Where public-sector data in Wales or England is held in UK data centres but processed using software or services from foreign-headquartered providers, operational control, audit, insider access and exit arrangements therefore deserve at least as much scrutiny as the location of the servers.

The author intends to put the following question in writing to the Welsh Government Cabinet Secretary with responsibility for health and social care, copied to the minister responsible for digital and data policy:

'Do NHS Wales bodies, Digital Health and Care Wales or the Welsh Government

1. use, pilot or intend to procure data-analytics or data-platform software supplied by Palantir Technologies or any other US-headquartered provider for identifiable patient or citizen data;
2. if so, who is the data controller, where is the data processed and backed up, what assessment has been made of exposure to the United States CLOUD Act, and what exit arrangements exist?'

No answer to a question in these terms has been identified. A request via WhatDoTheyKnow to Digital Health and Care Wales for any such contracts and data protection impact assessments could follow once a reply is received.

And another proposed to go to Kanishka Narayan MP, as Minister for Artificial Intelligence, asking that it be passed to the Secretary of State for Health and Social Care if the first part falls to that department:

> 'Will the Government accept the Science, Innovation and Technology Committee's recommendation to exercise the February 2027 break

[152] Wired, 'Palantir is helping DOGE with a massive IRS data project' (April 2025), as summarised by beSpacific (12 April 2025). https://www.bespacific.com/?p=112372

clause in the NHS Federated Data Platform contract; and what contingency plans has the Government made in case a US-headquartered provider of public-sector data infrastructure is compelled, under the CLOUD Act or otherwise, to give access to UK data or to withdraw its services?'

A request via WhatDoTheyKnow to NHS England for the exit plan for the Federated Data Platform contract could be a natural follow-up.

Control of computing power, not only of data

The questions above concern data. A parallel set of questions concerns computing capacity itself.

As one commentator has put it, 'Ownership, operating rights and contractual access decide who can use the machines - not the building's postcode.'[153] Four recent developments suggest that this is a practical rather than a theoretical concern.

First, the Government's plan for AI Growth Zones, published in November 2025, offers developers faster planning decisions, priority for grid connections and, in some regions, discounted electricity.

It states that 'onshore data centre capability is essential for protecting sensitive data' and that the Government's approach 'will ensure we have the ability to act independently and effectively where it matters most', while accepting that 'certain AI (artificial intelligence) workloads can and will be serviced offshore'.

This appraisal has found nothing in it requiring operators, in return for those advantages, to give the United Kingdom any right to reserve computing capacity in an emergency, to disclose who their customers are or what works is done, or to observe any restriction on foreign ownership or on foreign military or intelligence use.[154]

The private partnership announced for the North East AI Growth Zone, Stargate UK, is described by OpenAI as strengthening the United Kingdom's 'sovereign compute capabilities', although it involves privately owned companies, two of them headquartered in the United States.[155]

---

[153] Nation.Cymru, 'AI Minister Kanishka Narayan criticised in new book' (9 October 2026), quoting the author Thomas Vale. https://nation.cymru/news/ai-minister-kanishka-narayan-criticised-in-new-book/

[154] Department for Science, Innovation and Technology, 'Delivering AI Growth Zones' (policy paper, 13 November 2025). https://www.gov.uk/government/publications/delivering-ai-growth-zones/delivering-ai-growth-zones

[155] OpenAI, 'Introducing Stargate UK' (16 September 2025), with NVIDIA and Nscale; see also Department for Science, Innovation and Technology, 'North East England set for billions in investment and thousands of jobs as UK and US ink tech partnership' (September 2025), confirming that Cobalt Park forms part of the North East AI Growth Zone. https://openai.com/index/introducing-stargate-uk/; https://www.gov.uk/government/news/north-east-england-set-for-billions-in-investment-and-thousands-of-jobs-as-uk-and-us-ink-tech-partnership

In June 2026 a decision taken in another country switched off advanced AI services for users in the United Kingdom.

On 12 June the United States Government directed that two of Anthropic's most advanced models, Fable 5 and Mythos 5, must not be made available to non-US nationals. Because it could not check users' nationality in real time, Anthropic suspended both models for all customers worldwide. The company complied while publicly disagreeing with the directive, which was lifted on 30 June, with access returning from 1 July.[156,157]

One analyst observed that spreading services across several cloud providers does not protect a user against action taken against the model provider itself.[158] Where a service is switched off at source, it makes no difference in which country's data centre it would otherwise have run.

Independent safety testing depends on suppliers' cooperation. The Financial Times reported in September 2026 that the UK AI Security Institute was not given access to Anthropic's Mythos 5.1 before its release, although the Institute had evaluated earlier Anthropic models. The Government said that the Institute 'continues to work closely with industry partners, including Anthropic'.[159]

Much of the capacity being built is dual-use. Several of the companies building or using AI infrastructure in the United Kingdom also serve the United States defence establishment. OpenAI, for example, was awarded a $200 million US Department of Defense contract in June 2025.[160] This appraisal has not identified any published requirement, for AI Growth Zones or more generally, that would prevent capacity on UK sites, built with the benefit of UK planning and grid priority, from being used for another state's military or intelligence work, or that would allow the UK Government to know whether it is.

What follows is the author's own inference, not a finding of any of the sources cited.

'Sovereign' capacity should mean capacity over which the United Kingdom has enforceable rights: to call on it in an emergency, to prevent it from being

[156] Anthropic, 'Statement on the directive to suspend Fable 5 access' (12 June 2026). https://www.anthropic.com/news/fable-mythos-access

[157] CIO, 'US reverses export restrictions on Anthropic's Fable 5, Mythos 5 AI models' (30 June 2026). https://www.cio.com/article/4191550/us-reverses-export-restrictions-on-anthropics-fable-5-mythos-5-ai-models.html

[158] See n 157 above.

[159] ITPro, 'Anthropic reportedly withholds access to Mythos 5.1 from UK safety testing body' (9 September 2026), reporting the Financial Times; see also The Next Web, 'Anthropic kept Mythos 5.1 from the UK's AI safety testers' (10 September 2026). https://www.itpro.com/technology/artificial-intelligence/anthropic-reportedly-withholds-access-to-mythos-5-1-from-uk-safety-testing-body; https://thenextweb.com/news/anthropic-mythos-5-1-uk-aisi-pre-release-testing-withheld

[160] Bloomberg, 'OpenAI Snags $200 Million Contract With US Defense Department' (17 June 2025). https://www.bloomberg.com/news/articles/2025-06-17/openai-snags-200-million-contract-with-us-defense-department

directed by another government against UK interests, and to know, at least by category, who uses it and for what. Such rights could be made conditions of the planning, grid and energy advantages now on offer, but they do not appear to have been sought. As with water and energy, the remedy is disclosure and enforceable terms, so that the public can see what is being obtained in return for public advantages.

Similar considerations apply to the public money now committed to AI. The Government has told Parliament that the Managing Partner of the £500 million Sovereign AI Fund was appointed through a competitive civil-service process in which ministers had no role, and that she is recused from decisions involving real or perceived conflicts of interest.[161] Given the number of public and private roles that now touch AI investment, procurement and data-centre policy, a single published account of how conflicts of interest are recorded and managed across that field, for ministers, officials and fund managers alike, would strengthen public confidence.

The author intends shortly to put the following questions in writing to Kanishka Narayan MP, as Minister for Artificial Intelligence. First:

> 'What does the Government mean by sovereign AI capability in practice, and will it attach enforceable conditions to the planning, grid and energy advantages given to AI Growth Zones, including a right for the United Kingdom to reserve capacity in an emergency, a requirement that operators do not give another government's directions priority over their contracts with UK public bodies, disclosure to the Government of customer nationality and workload categories, and notification or prohibition of foreign military and intelligence workloads?'

A request via WhatDoTheyKnow to the Department for Business, Innovation, Science and Trade for any agreements or heads of terms with AI Growth Zone operators would show whether any such terms exist if no response is forthcoming.

Secondly:

> 'Following the United States directive of June 2026 that removed access to two AI models for all non-US nationals, what assessment has the Government made of the exposure of UK public services and businesses to foreign export-control and similar decisions affecting AI services and computing capacity, and what contingency arrangements are in place?'

A request via WhatDoTheyKnow for any such assessment could follow, although national-security exemptions may well be claimed.

---

[161] UK Parliament, written question on Sovereign AI Unit appointments, answered 22 May 2026. https://www.parallelparliament.co.uk/question/864/sovereign-ai-unit-public-appointments

Thirdly:

> 'Will the Government seek a statutory or contractual right for the AI Security Institute to test the most capable AI models before their release, given reports that it was not given pre-release access to Mythos 5.1?'

No answer to a question in these terms has been identified.

Fourthly:

> 'Will the Government publish a single account of how conflicts of interest are recorded and managed across AI investment, procurement and data-centre policy, including for ministers, officials and those managing the Sovereign AI Fund?'

A request via WhatDoTheyKnow to the Cabinet Office for the guidance applied could follow; records about individuals are likely to be withheld as personal data.

13. Regulatory Stability and International Confidence

International transfer frameworks depend not only upon legal rules but also upon confidence in the institutions responsible for implementing them.

The United Kingdom currently maintains adequacy arrangements and transfer mechanisms designed to support lawful international transfers, including transfers involving participating organisations in the United States.[162,163]

Recent developments in the United States, including the Supreme Court decision in *Trump v Slaughter*, have prompted discussion among some observers regarding wider questions of institutional governance and regulatory stability. However, the case was not a data-protection case and did not alter UK GDPR, UK adequacy regulations or existing UK-US transfer arrangements.[164]

Its relevance, if any, lies within broader discussions concerning institutional confidence rather than direct changes to data-protection law. However, it does demonstrate a weak link waiting to be broken and raising the question whether there is a GDPR-proof pipeline that is sufficiently solid for use at this time.

Sovereignty by dependence: a discussion point

Sections 9 to 13 above consider the legal mechanisms that govern where data is held and who may lawfully see it.

A further question, more speculative but potentially more important, is offered here as a point for discussion rather than as a finding. Whether, by allowing so much of the data belonging to their citizens, businesses and public institutions to be held by a small number of companies headquartered in another state, Western host nations have in practice ceded part of their sovereignty to that state - not by any treaty or deliberate decision, but by dependence.

The mechanism is simple to state.

A company remains subject to the laws of the state in which it is headquartered, wherever its servers happen to be.

If that state requires the company to produce, copy or withhold data, the company faces conflicting obligations. UK data protection law offers less protection here than is sometimes assumed. Article 48 of the EU GDPR provides that a judgment or decision of a court or authority outside the EU

[162] See n 135 above (ICO, Adequacy Regulations).
[163] See n 136 above (ICO, UK Extension to the EU-US DPF).
[164] Trump v Slaughter, 609 U.S. ___ (2026). The decision concerned presidential removal powers relating to FTC commissioners and did not alter UK GDPR, adequacy regulations or UK-US transfer arrangements. https://supreme.justia.com/cases/federal/us/609/25-332/

requiring personal data to be transferred or disclosed may be recognised or enforced only if it is based on an international agreement. The equivalent article was omitted from the UK GDPR when the Brexit transition period ended on 31 December 2020, so UK law now contains no express rule of that kind. A company asked by a foreign authority to hand over personal data held here must still comply with the general UK GDPR rules on transfers abroad, but there is no specific bar on giving effect to the foreign order.

Even in the EU, the protection binds the company, not the foreign state, and it works only if the company is willing and able to refuse. Where the penalty for defying its home state is heavier than the penalty for breaching the host nation's data protection law, the host nation's law may in practice give way.

A senior representative of one major cloud provider, asked under oath by a French Senate inquiry in June 2025 whether he could guarantee that French citizens' data would not be transmitted to a foreign government without French consent, answered that he could not, while adding that it had never happened.[165,166]

Nor is this a matter of hypothesis so far as the law is concerned. At least two of the world's largest economies already have laws under which their authorities can require companies within their jurisdiction to produce data held abroad, or to support, assist and cooperate with state intelligence work. This appraisal deliberately does not single out any one state in the text: the point is structural, and would apply to whichever state is home to the companies on which a host nation comes to depend.[167]

Legal compulsion is not the only lever.

A powerful state can also apply financial pressure, through sanctions or penalties directed at the companies themselves or at those they serve.

---

[165] EU GDPR, Article 48 ('Transfers or disclosures not authorised by Union law'), under which a judgment or decision of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforced if based on an international agreement (second link). The corresponding article of the UK GDPR was omitted with effect from 31 December 2020 by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419), Schedule 1, paragraph 41; only its heading remains on the UK legislation database (first link). https://www.legislation.gov.uk/eur/2016/679/article/48; https://gdpr-info.eu/art-48-gdpr/

[166] The Register, 'Microsoft admits it cannot guarantee data sovereignty' (25 July 2025), reporting the evidence of Anton Carniaux, Microsoft France's director of public and legal affairs, to a French Senate inquiry on 18 June 2025, in the context of the United States CLOUD Act. https://www.theregister.com/2025/07/25/microsoft_admits_it_cannot_guarantee/

[167] Examples include the United States CLOUD Act 2018 (see n 166 above) and Articles 7 and 14 of the National Intelligence Law of the People's Republic of China (2017, amended 2018), Article 7 of which provides that 'all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law'. The examples are given to show that the issue is not confined to one state. https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

One recent episode illustrates the point, although it concerns access to a service rather than access to data.

After sanctions were imposed by one state on officials of the International Criminal Court in 2025, the Court's chief prosecutor was disconnected from the email service provided by a major technology company. That company first told a UK parliamentary committee that the disconnection had been the Court's own decision, and in February 2026 apologised and asked for the record to be corrected, stating that it had been in touch with the Court throughout the process that resulted in the disconnection.

The Court has since begun moving to open-source software provided through a European public body. An international institution's dependence on a single foreign provider was, in other words, capable of being turned against it by a third state's financial measures.[168,169]

Access may also be obtained without any open demand at all.

In 2020 the Court of Justice of the European Union, invalidating an earlier transatlantic data transfer arrangement, found that the surveillance programmes of the state concerned were not limited to what is strictly necessary and did not give the people affected rights they could enforce in court.

Read with the material above, this suggests a sliding scale. How a powerful state might obtain material held by its own companies - by negotiated agreement, by legal compulsion, by financial pressure, or covertly - is likely to depend on the difference in power between that state and the host nation, and on how much the material matters to it. The host nation will often not know which, if any, has occurred.[170]

A further possibility, which this appraisal has not seen in force anywhere and offers purely as its own inference, is that the state in which a custodian of another nation's data is based could in future legislate to require that custodian to copy that state in to data it holds, or to give that state's own businesses, investigators or agencies access to it, for commercial as well as

[168] The Register, 'Microsoft throws spox under the bus in ICC email flap' (18 February 2026), reporting Microsoft's apology to the House of Commons Business and Trade Committee and its request that the record be corrected; see also Computer Weekly, 'Microsoft's ICC email block reignites European data sovereignty concerns' (23 May 2025). https://www.theregister.com/2026/02/18/microsoft_asks_uk_parliament_to_correct_record/; https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns

[169] The Register, 'International Criminal Court dumps Microsoft Office' (31 October 2025), reporting the Court's move to openDesk, an open-source suite provided by Germany's Centre for Digital Sovereignty (ZenDiS) on behalf of the German Federal Ministry of the Interior. https://www.theregister.com/software/2025/10/31/international-criminal-court-dumps-microsoft-office/680564

[170] Court of Justice of the European Union, Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems ('Schrems II'), judgment of 16 July 2020; Court press release No 91/20. https://curia.europa.eu/site/upload/docs/application/pdf/2020-07/cp200091en.pdf

security purposes. Nothing in the present arrangements identified in this appraisal would prevent such a law being passed, and a host nation's practical remedies once it was passed - other than moving its data elsewhere, at great cost and over many years - appear limited.

Some host nations have begun to respond.

France's SecNumCloud qualification for cloud services used by sensitive public bodies includes requirements intended to protect against the reach of non-European laws, including limits on non-European ownership and control.

Denmark's ministry for digitalisation announced in 2025 that it was moving its staff from proprietary office software to open-source alternatives, citing digital independence.

The United Kingdom has taken a different route. Its Data Access Agreement with one major partner state, in force since October 2022, creates a negotiated channel through which each country's authorities can make requests directly to service providers in the other, subject to safeguards - an approach that regulates access rather than preventing it. This appraisal has not identified any UK or Welsh Government policy that assesses the risk described in this section for public-sector or citizens' data held by foreign-headquartered providers, nor any requirement comparable to SecNumCloud. The point has particular force where, as at Bro Tathan (Section 16 below), a foreign-headquartered operator's infrastructure is sited on land owned by government itself.[171,172,173]

None of this suggests that any company has acted unlawfully, or that data belonging to people in Wales or England has been disclosed in the ways described; the companies concerned state that they resist requests they consider unfounded. The risk is of low probability but high consequence, and once data has been taken it cannot be recovered. That is precisely the kind of risk to which the precautionary principle discussed in Section 17 below is directed. The question this appraisal asks is therefore not whether the risk will materialise, but what host nations are doing about it.

---

[171] BSA | The Software Alliance, comments to ANSSI on SecNumCloud version 3.2 (15 November 2021), objecting to its 'immunity to extraterritorial legislation' requirements; for a summary of the requirements, including limits of 24% individually and 39% collectively on non-EU shareholdings, see Scalingo, 'SecNumCloud qualification (ANSSI): complete guide' (a cloud provider's guide, not an official source). https://www.bsa.org/policy-filings/france-bsas-comments-to-anssi-on-secnumcloud-version-32a; https://scalingo.com/blog/secnumcloud-qualification-anssi-guide

[172] The Record, 'Danish government agency to ditch Microsoft software in push for digital independence' (June 2025), quoting the Danish Minister for Digitalisation, Caroline Stage Olsen. https://therecord.media/denmark-digital-agency-microsoft-digital-independence

[173] eucrim, 'UK-US E-Evidence Agreement in Force', reporting the entry into force of the UK-US Data Access Agreement on 3 October 2022. https://eucrim.eu/news/uk-us-e-evidence-agreement-in-force/

A suggested question, which the author intends to put in writing to the Welsh Government minister responsible for digital and data policy, and in parallel to Kanishka Narayan MP as Minister for Artificial Intelligence, asking him to pass it to the responsible minister if digital and data policy falls elsewhere, reads:

> 'What assessment has the Government made of the risk that data held for public bodies, businesses and citizens in Wales [the United Kingdom] by companies headquartered in another state could be accessed, copied or withheld as a result of that state's laws, sanctions or financial pressure on those companies, rather than under Welsh or UK law; and what safeguards - for example, requirements comparable to France's SecNumCloud qualification - are in place or under consideration for public-sector data, including data held at facilities such as Bro Tathan?'

No answer to a question in these terms has been identified in the Senedd Record, Hansard or via WhatDoTheyKnow to date. A freedom of information request via WhatDoTheyKnow to the Welsh Government and to Digital Health and Care Wales, seeking any risk assessment of foreign-law exposure in their principal cloud contracts, could be a useful parallel step; any answer received could then be compared with the safeguards adopted in France and Denmark.

14. Resilience, Backup and Systemic Risk

Modern society increasingly depends upon a complex ecosystem of digital infrastructure.

Industry practice commonly relies upon:

- geographic redundancy;
- multiple copies of data;
- disaster-recovery facilities;
- distributed architecture;
- availability zones.

These measures are designed to reduce single points of failure and improve continuity of service.

Important questions remain:

- How geographically dispersed should backups be?
- Should some information remain within specified jurisdictions?
- How should resilience be balanced against sovereignty considerations?
- Does increasing dependence upon a relatively small number of cloud providers create systemic risks?

These remain active areas of discussion rather than settled questions.[174,175]

[174] See n 5 above (HoC Library, CBP-10315).
[175] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).

15. Regional Concentration and Proliferation Effects

London and Slough

London and the South East remain the principal concentration of data-centre infrastructure within Great Britain.

Official statistics indicate that Slough accounted for approximately 29% of British data-centre electricity consumption in 2024 and that data centres represented around 65% of local grid electricity use.[176]

This concentration has prompted discussion concerning:

- electricity-network capacity;
- water resources;
- cumulative environmental impacts;
- infrastructure dependency.[177,178]

There is little settled evidence yet on how quickly this concentration might translate into a visible supply problem, but comparable experience elsewhere offers some indication of the pace at which regional strain can develop, and of what other jurisdictions have found it useful to monitor.

In Ireland, data centres' share of national electricity demand rose from around 5% in 2015 to 22% by 2024, prompting a four-year moratorium on new data-centre grid connections that was lifted only in December 2025, and then on condition that new facilities provide their own back-up generation or storage capacity and source 80% of demand from renewable energy within six years.[179]

In Northern Virginia's 'Data Center Alley', average data-centre water use in the Washington DC metropolitan area is projected to rise roughly fourfold between 2025 and 2035, with researchers there calling for mandatory monthly water-use reporting that does not yet exist, on the basis that current voluntary disclosure is inadequate to plan for the change.[180]

The Netherlands and Singapore have each, at different times, imposed their own pauses on new hyperscale development - the former to allow local consultation to catch up with the pace of proposals, the latter over energy

[176] See n 7 above (DESNZ, Data Centre Electricity Consumption).
[177] See n 7 above (DESNZ, Data Centre Electricity Consumption).
[178] See n 10 above (HoC EAC, Risks and Opportunities Inquiry).
[179] Pinsent Masons, 'New Irish Data Centres Must Generate Power Back into National Grid, Rules Regulator', reporting the Commission for Regulation of Utilities' final policy decision of December 2025. https://www.pinsentmasons.com/out-law/news/irish-data-centres-power-national-grid-regulator
[180] Frontier Group, 'Does Virginia Have Enough Water to Quench Thirsty Data Centers?' (2026). https://frontiergroup.org/articles/does-virginia-have-enough-water-to-quench-thirsty-data-centers/

consumption and emissions - before both later reopened development under stricter efficiency and renewable-energy conditions.[181,182]

Applying that experience to London and the South East, the material identified in the course of this appraisal does not permit a confident prediction of exactly when accumulated demand might translate into a visible shortage.

What can be said is that the region's water stress is already classified as serious by the Environment Agency, rather than merely anticipated, and that indicators used elsewhere to identify pressure - a grid operator or regulator publicly warning that connection requests exceed available capacity, as Ofgem has already done in relation to parts of Wales;[183] a water company setting out demand-side restrictions specific to data centres, as Thames Water has begun to explore; and a rising share of a local authority's total electricity or water demand attributable to data centres, as already measured for Slough above - are either present, or beginning to appear, in London and the South East now, rather than at some more distant point in the future.

Whether that combination is treated by government and regulators as an early warning meriting closer monitoring, in the way Ireland's rise from 5% to 22% grid share eventually was, is, in the authors' assessment, one of the more pressing open questions this appraisal identifies.

This assessment draws together evidence from several jurisdictions rather than resting on a single source, and readers should treat it as an informed extrapolation rather than an established finding.

South Wales

South Wales is emerging as one of the principal growth areas outside London.

Major proposals in Cardiff, Newport and Bridgend have created opportunities for investment and skills development while also raising questions regarding infrastructure demand, biodiversity, water resources and long-term community benefit.[184]

---

[181] Data Center Dynamics, 'The Netherlands' Hollands Kroon Wants to Pause Hyperscale Data Center Developments' (30 June 2022). https://www.datacenterdynamics.com/en/news/the-netherlands-hollands-kroon-wants-to-pause-hyperscale-developments/

[182] Lexology, 'Building Green Data Centres - Singapore Lifts Moratorium on New Data Centres, Introduces Environmental Sustainability Standards', summarising Singapore's 2019-2022 moratorium and its March 2022 conditions for new capacity. https://www.lexology.com/library/detail.aspx?g=254ea4fc-98b1-465f-9904-2f4c4c3496fc

[183] Fuse Energy, analysis of electricity demand from proposed Welsh data centres and the South Wales AI Growth Zone, citing Ofgem's warning that the current network cannot accommodate all proposed data-centre grid connections (2026). https://www.fuseenergy.com/news/welsh-data-centre

[184] See n 20 above (Senedd Research, Data Centres in Wales).

These discussions are likely to become increasingly important as Welsh digital infrastructure continues to expand.[185]

Some indication of the pace of change already exists.

Proposed data-centre developments across Wales, taken together with the South Wales AI Growth Zone, could require additional generating capacity of around 1.4 gigawatts - nearly ten times current operational data-centre capacity in Wales - and the AI Growth Zone alone has been estimated to require some 13% of Wales's total electricity generating capacity by the early 2030s.

Ofgem has itself warned that the current electricity network cannot accommodate all proposed data-centre connections being sought.[186]

As with London and Slough, this appraisal has not identified a published, Wales-specific equivalent of the Environment Agency's water-stress classifications, or of Thames Water's demand projections, that would allow the water dimension of this growth to be assessed with the same degree of evidence; that absence of comparable data is itself one of the gaps this appraisal identifies.

[185] See n 20 above (Senedd Research, Data Centres in Wales).
[186] See n 183 above (Fuse Energy, Welsh data centres and grid capacity).

16. Bro Tathan: Public Land, a US Operator and Unresolved Governance Questions

One proposal illustrates several of the tensions discussed elsewhere in this appraisal with particular clarity.

Vale of Glamorgan Council has granted planning consent for a substantial data-centre campus at Bro Tathan, on the site of the former RAF St Athan airfield, to be developed by Vantage Data Centers under a 999-year lease of Welsh Government-owned land.[187,188,189]

Vantage is a US-headquartered operator, and the Welsh Government has indicated that the development forms part of a wider, multi-billion-pound programme across its South Wales campuses - including Newport, Bridgend and Bro Tathan - expected to exceed 1GW of AI-ready capacity, with Ministers publicly welcoming the investment as a source of high-skilled employment and as central to the South Wales AI Growth Zone.[190]

This arrangement places the Welsh Government in an unusually direct set of overlapping roles: it is the freeholder leasing the land, an active promoter of the investment through its AI Growth Zone and economic-development strategy, and, separately, ultimately answerable for the planning and data-governance framework within which the development is assessed.

The commercial terms of the lease itself do not appear to have been made widely public.[191] Given that the same development places a US-headquartered operator's infrastructure on land owned directly by a devolved government, the sovereignty and jurisdiction questions considered in Sections 9 to 14 above - UK GDPR adequacy, exposure under the US CLOUD Act, and the adequacy of existing international transfer mechanisms - arise here in a sharper and more immediate form than in relation to data-centre development generally.

It would be preferable for the Welsh Government's position on these points, and on how it manages the potential conflict between its landowner and promotional interests on one hand and its regulatory and public-data responsibilities on the other, to be stated clearly and resolved before, rather than after, such developments are committed.

---

[187] CarneySweeney, Vantage Data Centre, Bro Tathan, Vale of Glamorgan — planning consent summary. https://www.carneysweeney.co.uk/projects/vantage-data-centre-bro-tathan-vale-of-glamorgan.html

[188] Baxtel, Vantage: Bro Tathan CWL2 Data Center — site profile confirming the 999-year Welsh Government lease and US ownership. https://baxtel.com/data-center/vantage-bro-tathan-cwl2

[189] Welsh Government, Bro Tathan — Cardiff Airport and Bro Tathan Enterprise Zone. https://www.gov.wales/bro-tathan

[190] Vantage Data Centers, Vantage Data Centers and Nebius Expand UK AI Infrastructure with First Deployment in South Wales AI Growth Zone (2026). https://vantage-dc.com/news/vantage-data-centers-and-nebius-expand-uk-ai-infrastructure-with-first-deployment-in-south-wales-ai-growth-zone/

[191] See n 188 above (Baxtel, Bro Tathan CWL2 profile).

The same questions arise at Bro Tathan in relation to computing capacity (see 'Control of computing power, not only of data' in Section 12 above). The site forms part of the South Wales AI Growth Zone, and it is not known whether the lease, or any agreement connected with the Growth Zone, gives the Welsh or UK Government any right to reserve capacity on the site in an emergency, or any information about, or say over, the customers it serves and the work done there.

The author intends to put the following question in writing to the Welsh Government Cabinet Secretary responsible for the economy, as landowner:

> 'Does the lease to Vantage Data Centers at Bro Tathan, or any related agreement, give the Welsh or UK Government any right to reserve computing capacity in an emergency, or any information about, or control over, the customers served and the work carried out on the site?'

A request via WhatDoTheyKnow for the lease and related agreements could follow; commercial confidentiality is likely to be argued, but the public-interest test applies.

What the screening file shows (October 2026)

In October 2026 Vale of Glamorgan Council released, in response to the author's request via WhatDoTheyKnow, its file on whether the Bro Tathan data centre needed an environmental impact assessment.[192] The documents, which are public on that site, add a good deal to the history set out above. What follows describes them; comments that are the author's own are identified as such.

In January 2022 the applicant's planning consultants, CarneySweeney, asked the Council on behalf of Vantage Data Centers for a screening opinion (whether an assessment was needed) and a scoping opinion (what it should cover) for a phased data centre of up to about 83,000 square metres on 11.3 hectares. The request said that the development 'is unlikely to have significant environmental impacts', that the use of water 'will be very slight', and that standby generators of 2.6 MW each would run only in emergencies and for about 18 hours a year of testing. It did not address the facility's demand for electricity, the water needed for cooling or its carbon emissions.[193] The request described 11 generators for each pair of data halls, across up to six phases of two data halls each; read literally, that suggests

[192] Vale of Glamorgan Council, response of 16 October 2026 (reference 00211434) to the author's request 'Screening of Datacentre at Bro Tathan' made via WhatDoTheyKnow on 11 September 2026, with 18 attachments. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t

[193] CarneySweeney for Vantage Data Centers, 'Environmental Impact Assessment - request for screening and scoping opinion', letter to Vale of Glamorgan Council (13 January 2022), applications 2022/00038/SC1 and 2022/00084/SC2, pages 3, 6 and 9. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/17/220113%20EIA%20Screening%20Scoping%20Request.pdf.html

up to 66 generators, whereas the Council's report later described three buildings with 11 generators each. Neither document states a total; this is the author's reading. The accompanying plan labelled the buildings 32 MW, 32 MW, 16 MW and 16 MW.[194]

On 8 February 2022 the Council's senior planner told the consultants informally, before consultation responses had been received, that 'it is likely that the proposals would require an EIA, although the scope of which may be relatively limited', covering landscape, heritage, transport, ground conditions, noise and air quality, and ecology. The consultants disputed that the same day and the next, relying on guidance in Welsh Office Circular 11/99 that assessment is 'more likely to be required' for industrial estates of more than 20 hectares, and saying that they were 'genuinely struggling to see' any likely significant effects.[195]

On 17 February 2022 the Council issued its screening opinion: an environmental impact assessment was not required. The officer's report noted that the wider allocated site 'cumulatively would far exceed the threshold' and that 'the accumulation of effects needs to therefore be carefully considered', but concluded that the effects would be of local significance only. It recorded that no comments had yet been received from the Council's highways, drainage, pollution control and ecology consultees, and it accepted that the generators 'would only be utilised in extreme circumstances'. Because no assessment was required, the accompanying request for a scoping opinion was closed without a response.[196,197]

A month later, on 14 March 2022, the consultants sent the Council a summary of their own Phase I environmental site assessment. It recorded that the southern part of the site had been used as a fire-training ground, that residual contamination of soil and groundwater 'is likely to be present beneath the site, including per- and polyfluoroalkyl substances (PFAS), used in fire-fighting foam', together with hydrocarbons and possibly asbestos,

---

[194] Scott Brownrigg, 'St Athan Data Centre Proposal: areas and dimensions' (December 2021), submitted with the screening request. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/14/St%20Athan%20Data%20Centre%20Proposal%20Site%20Plan%20A1%20Updated.pdf.html

[195] Email exchange between Vale of Glamorgan Council planning officers and CarneySweeney, 8 and 9 February 2022 ('RE: Data Centre, Bro Tathan'). https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/9/RE%20Data%20Centre%20Bro%20Tathan.html

[196] Vale of Glamorgan Council, screening report 2022/00038/SC1 and decision notice of 17 February 2022. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/3/2022%2000038%20Final%20Report%20202200038SC1.pdf.html; https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/24/R%202022%2000038%20Decision%20Notice%20202200038SC1.pdf.html

[197] Vale of Glamorgan Council, internal email closing scoping request 2022/00084/SC2. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/19/2022%2000084%20SC2.html

that nine buried radium-containing objects had been found, that the site lies over a Secondary A aquifer with drainage channels flowing to the Boverton Brook, and that the layout encroached on a flood-defence bund and a designated flood-storage area.[198] The Council's land-quality advisers had already noted, on the scoping file, potential risks from 'made ground, radioactive material and fuel tanks'.[199]

The planning application eventually approved, 2023/00780/FUL, as amended in March 2024, covers about 26.7 hectares, of which about 12.6 hectares is the building and related development, with a building of 67,227 square metres and 72 diesel generators able to produce 120 MW in total. Natural Resources Wales initially said that it would object unless more information was provided on land contamination and protected species; it noted that the planning boundary then included 'an area known to be where firefighting practice of fighter jets took place and was the main perfluoroalkylated (PFAS) source area', and that 'all locations where PFAS has been detected exceed the adopted screening criteria'. The boundary was later redrawn to exclude most of the fire-training area, and the Council's advisers noted that land retained by the Welsh Government was 'not addressed by the remediation strategies submitted to date'. The application proposed 120 full-time jobs, against the 216 described in 2022; the report itself observed that a typical storage or industrial building of the same size would support about 1,003.[200]

On the question of assessment, the report relied on the 2022 opinion, describing the proposal as 'essentially the same use' and 'a building covering a similar area', 'largely commensurate in terms of the material considerations', and concluded that no assessment was required. Neither the 2022 screening report nor the 2024 committee report contains an assessment of the electricity the data centre would draw or of the water used for cooling.[201]

In the author's view, the file illustrates the points made in Section 2 and in the discussion of environmental assessment elsewhere in this appraisal. The decision that no assessment was needed was taken early, on the

---

[198] CarneySweeney, email to Vale of Glamorgan Council of 14 March 2022, 'Data Centre, Bro Tathan', section 'A summary of the survey work being undertaken'. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/25/R%20200322%201234.pdf.html

[199] Shared Regulatory Services, land-quality memorandum on 2022/00084/SC2 (dated 2 February 2021 on its face; ref SRS/E/10875/22). https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/4/2022%2000084%20202200084SC2.pdf.html

[200] Vale of Glamorgan Council, report to Planning Committee on application 2023/00780/FUL, Land North of Ffordd Bro Tathan (2024), including 'Need for Environmental Impact Assessment', the generators, staffing and the responses of Natural Resources Wales and Shared Regulatory Services. https://www.whatdotheyknow.com/request/screening_of_datacentre_at_bro_t/response/3594738/attach/html/20/Final%20Report%20202300780FUL%201%20compressed.pdf.html

[201] See n 200 above.

applicant's description of a smaller site, before the main consultees had replied and before the contamination of the site was set out; and it was then carried forward to a scheme on more than twice the area, with a known PFAS source area inside its first boundary and 120 MW of diesel generation. No impropriety is suggested by this appraisal, and whether the law required a fresh screening opinion is a question for others; legal remedies are not considered here. What the file does show is how the questions that matter most for data centres - power, water, chemicals and cumulative effect - can fall outside the process altogether.

The author intends to put the following question in writing to Vale of Glamorgan Council's Head of Sustainable Development: 'Was a screening opinion adopted under the Town and Country Planning (Environmental Impact Assessment) (Wales) Regulations 2017 specifically for application 2023/00780/FUL, as distinct from reliance on the 2022 opinion for a smaller site? If so, please provide it and say whether it took account of the enlarged site of about 26.7 hectares, the former fire-training area identified by Natural Resources Wales as the main PFAS source area, and the 72 standby generators with a combined capacity of 120 MW.' A request via WhatDoTheyKnow for any screening record or officer notes for that application could follow.

And to the Welsh Government Cabinet Secretary responsible for the economy, as landowner: 'The Council's report on application 2023/00780/FUL records that land at Bro Tathan retained by the Welsh Government is not addressed by the remediation strategies submitted. What assessment has the Welsh Government made of PFAS contamination of soil and groundwater on its retained land there, including the former fire-training area, what remediation is planned, and who will pay for it? And before granting the lease, what due-diligence, environmental and data-protection assessments did the Welsh Government carry out, and how did it keep its roles as landowner, promoter of the investment and regulator separate?' Requests via WhatDoTheyKnow to the Welsh Government for those assessments, and to Natural Resources Wales for any monitoring of PFAS in groundwater beneath the site and in the Boverton Brook, could follow.

17. Artificial Intelligence: Warnings, Uncertainty and the Precautionary Principle

This appraisal has so far treated artificial intelligence primarily as the driver of data-centre demand.

A fuller appraisal cannot avoid a harder question: a number of the people building the most advanced AI systems, including staff at Anthropic, have themselves warned publicly that the technology could pose extreme risks, up to and including loss of human control over decisions that matter to survival.

Whatever view is taken of these warnings, their source - not campaigners or outside critics, but researchers and executives within the leading AI developers - means they cannot responsibly be ignored in policy or planning terms.

In September 2026, several current and former Anthropic researchers, including its alignment-science lead, stated publicly that they assessed a meaningful probability of AI causing human extinction within a decade - in one case put at above ten per cent - while acknowledging that 'we do not yet have a plan to solve alignment for superintelligence'.[202]

Anthropic's chief executive, Dario Amodei, has separately warned of risks ranging from mass displacement of entry-level white-collar work to the potential for advanced AI to assist in the development of biological weapons, and has called for stronger governmental oversight of frontier AI development.[203]

These are not fringe views: in May 2023, leaders of Anthropic, OpenAI and Google DeepMind were among more than 100 signatories - alongside the Turing Award-winning computer scientists Geoffrey Hinton and Yoshua Bengio - of a one-sentence public statement that mitigating the risk of extinction from AI 'should be a global priority alongside other societal-scale risks such as pandemics and nuclear war'.[204]

Because several of the statements above come from people working at one company, Anthropic, it is right to record that comparable warnings come from sources independent of any AI developer. In his speech at the Nobel Prize banquet in December 2024, Geoffrey Hinton, joint winner of that year's Nobel Prize in Physics, warned of 'a longer term existential threat that will arise when we create digital beings that are more intelligent than ourselves', adding: 'We have no idea whether we can stay in control.'[205]

A peer-reviewed survey of 2,778 AI researchers, published in the Journal of Artificial Intelligence Research in 2025, found that between 38% and 51% of respondents gave at least a 10% chance to advanced AI leading to outcomes as bad as human extinction, even though a majority were, on balance, optimistic about advanced AI.[206]

---

[202] Axios, Anthropic Insiders Warn AI Could Kill All Humans (9 September 2026). https://www.axios.com/2026/09/09/anthropic-insiders-warn-ai-could-kill-all-humans

[203] Axios, Behind the Curtain: Anthropic's Warning to the World (26 January 2026). https://www.axios.com/2026/01/26/anthropic-ai-dario-amodei-humanity

[204] Center for AI Safety, Statement on AI Risk (30 May 2023). https://www.safe.ai/work/statement-on-ai-risk

[205] Geoffrey Hinton, banquet speech, Nobel Prize ceremony, Stockholm, 10 December 2024. https://www.nobelprize.org/prizes/physics/2024/hinton/speech/

[206] Katja Grace and others, 'Thousands of AI Authors on the Future of AI', Journal of Artificial Intelligence Research (2025), reporting a survey of 2,778 researchers who had published in leading AI venues, conducted in October 2023. https://www.jair.org/index.php/jair/article/view/19087

In October 2025 hundreds of scientists and public figures, including Hinton and Yoshua Bengio, signed a statement organised by the Future of Life Institute calling for 'a prohibition on the development of superintelligence, not lifted before there is broad scientific consensus that it will be done safely and controllably, and strong public buy-in'.[207]

The International AI Safety Report 2026, discussed below, is a further source independent of the companies concerned.

Governments have responded, if unevenly.

At the UK's AI Safety Summit at Bletchley Park in November 2023, 29 countries and the European Union, including the UK, the US and China, signed a declaration acknowledging the potential for serious, even catastrophic, harm from the most capable ('frontier') AI systems, and committing to international cooperation on safety testing and research.[208]

The UK went on to establish what is now the AI Security Institute to evaluate frontier models.

In Wales, the Senedd's Economy, Trade and Rural Affairs Committee reported in May 2025 that AI presented both substantial opportunity and serious risk to the Welsh economy - including, specifically, the energy and water demands of the data centres considered throughout this appraisal - and recommended that the Welsh Government map these risks and plan accordingly; the Welsh Government accepted all eight of the Committee's recommendations.[209]

None of this amounts to proof that catastrophic AI risk is likely, still less imminent.

Serious, well-informed people disagree sharply about probability and timescale, and this appraisal takes no view on who is right. What can be said is that the people with the deepest technical knowledge of these systems are not confident the risk is negligible, and say so openly.

That is precisely the condition in which the precautionary principle - long established in UK and Welsh environmental law and policy, including under the Environment Act 2021[210] and reflected in the duties underpinning Welsh

[207] Future of Life Institute, 'Statement on Superintelligence' (22 October 2025); for the date and initial signatories, see SiliconANGLE, 'Geoffrey Hinton, Yoshua Bengio sign statement urging suspension of AGI development' (22 October 2025). https://superintelligence-statement.org/; https://siliconangle.com/2025/10/22/geoffrey-hinton-yoshua-bengio-sign-statement-urging-suspension-agi-development/

[208] HM Government, The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

[209] Senedd Economy, Trade and Rural Affairs Committee, AI and the Welsh Economy: Can Welsh Androids Dream of Electric Sheep? (May 2025). https://laiddocuments.senedd.wales/cr-ld17182-en.pdf

[210] Environment Act 2021, section 17 (policy statement on environmental principles, including the precautionary principle). https://www.legislation.gov.uk/ukpga/2021/30/section/17

environmental governance - counsels action to prevent serious or irreversible harm even where scientific certainty is lacking, rather than waiting for proof before acting. Applied here, that suggests continued, well-resourced public scrutiny of frontier AI development, and of the infrastructure that supports it, rather than either alarmism or complacency.

There is a longer tradition behind this kind of thinking than either AI safety research or modern environmental law.

The 'seventh generation' principle, drawn from the Great Law of the Haudenosaunee (Iroquois) Confederacy, holds that the impact of a decision should be weighed against its consequences seven generations into the future.[211]

Wales has its own, more recent statutory expression of a closely related idea: the Well-being of Future Generations (Wales) Act 2015 requires public bodies, including the Senedd and Welsh Government, to act in a manner that seeks to ensure the needs of the present are met without compromising the ability of future generations to meet their own needs.[212]

Read together, these two traditions suggest that decisions about data-centre and AI infrastructure taken now - about energy, water, land and the underlying technology itself - should be judged not only by their economic case today, but by the world they leave behind for generations who have no voice in this appraisal, or in the planning decisions it discusses.

A number of further uncertainties fall outside the scope of this appraisal. They are noted briefly below as a bookmark for future consideration, rather than as matters this appraisal attempts to resolve:

- critical minerals and chip supply chains: the long-term availability and geopolitical security of the specialist minerals and semiconductors underpinning AI hardware are not addressed in this appraisal and remain uncertain;
- decommissioning and e-waste: little public information exists on what happens to data-centre hardware, and to the buildings themselves, at end of life, or on the electronic-waste and embodied-carbon consequences of the typically short (three-to-five-year) replacement cycle for AI-specific chips; that gap extends specifically to PFAS-containing fire-suppression and cooling systems, where this appraisal has identified no published UK or Welsh guidance on safe removal or disposal at decommissioning (see the discussion in Section 8 above);
- cumulative and combined effects: the individual assessments referred to throughout this appraisal are generally site-specific; the cumulative effect of multiple, geographically clustered developments on water

[211] Wikipedia, Seven Generation Sustainability, summarising the Haudenosaunee (Iroquois) Confederacy's Great Law principle. https://en.wikipedia.org/wiki/Seven_generation_sustainability

[212] See n 83 above (WFG (Wales) Act 2015 essentials).

catchments, grid capacity, biodiversity and local amenity together is much less well understood; and

- encryption and long-term data security: advances in quantum computing may, on some timescales, undermine the encryption standards on which current assumptions about data sovereignty and security depend; this appraisal does not attempt to assess that risk, but notes that it exists.

Beyond loss of control: deliberate misuse risks

The warnings considered above are framed mainly around the risk that an advanced AI system might itself pursue goals contrary to human welfare - the 'loss of control' or 'superintelligence' framing most associated with the 2023 Statement on AI Risk.

That framing is narrower than the risk landscape now used in international governance discourse. The International AI Safety Report 2026, chaired by Yoshua Bengio and backed by 30 governments, the OECD and the UN, treats 'malicious use' - a person or group deliberately directing a capable AI system to cause harm - as a distinct category of catastrophic risk, separate from malfunction or loss of control.

This appraisal follows that distinction: the risk is not only that AI might act against humanity on its own initiative, but that a person or group might use it as a tool to do so.[213]

One frequently discussed route is biosecurity: whether AI models can lower the barrier to designing or synthesising dangerous pathogens. The evidence here is genuinely mixed, and this appraisal presents both sides.

A RAND Corporation red-team study published in January 2024 found that the large language models then available did not meaningfully increase the risk of a biological weapons attack by a non-state actor, because their outputs largely mirrored information already available online.

Since then, however, frontier AI developers have themselves treated the risk as serious enough to warrant costly safeguards: Anthropic activated 'ASL-3' protections for its Claude Opus 4 model in May 2025, stating that it could not 'clearly rule out' the relevant risks and describing measures aimed specifically at preventing extended, end-to-end biological-weapons workflows, while OpenAI's Preparedness Framework tracks biological uplift as a 'High' capability category requiring active mitigation.

[213] International AI Safety Report 2026, chaired by Yoshua Bengio and backed by 30 governments, the OECD and the UN (January 2026), which structures its risk assessment around 'malicious use', 'malfunctions' and 'systemic risks' as distinct categories, separate from loss-of-control risk; see also Center for Security and Emerging Technology (Georgetown), 'How to Assess the Likelihood of Malicious Use of Advanced AI Systems' (March 2025). https://internationalaisafetyreport.org/publication/international-ai-safety-report-2026

Read together, this suggests that the risk, while not established as having already materialised, is being treated by those best placed to judge it as real and growing, rather than as a settled non-issue.[214,215]

A second route concerns nuclear command and control. This is a matter of documented expert concern rather than a documented incident: no publicly confirmed case of an AI system contributing to a nuclear near-miss is known to exist as of the date of this appraisal.

The Bulletin of the Atomic Scientists' 2026 Doomsday Clock Statement nonetheless set the Clock at 85 seconds to midnight, warning that AI may be embedded in nuclear decision-support systems and that 'a too-heavy dependence on black-box systems could present a serious danger'.

Specialist commentary uses the 1983 Petrov incident - in which a Soviet officer correctly judged a false satellite warning of a US missile launch to be an error, and declined to escalate - as the standard cautionary analogy for the risk that automation bias, or an unexplained AI-driven error (a 'glitch' in the terms this concern is often expressed in everyday language), could compress the time available for human judgement in a crisis and increase the risk of miscalculation.

Whether any state currently allows AI an operational role of that kind is not a matter on which this appraisal can offer a considered view; it notes the concern as expressed by specialists, not as an established fact about any particular system.[216,217]

Other deliberate-misuse vectors identified in the literature include

---

[214] RAND Corporation, 'Current Artificial Intelligence Does Not Meaningfully Increase Risk of a Biological Weapons Attack' (25 January 2024), a red-team study finding that the large language models tested did not, at that time, increase the risk posed by a non-state actor beyond information already available online. https://www.rand.org/news/press/2024/01/25.html

[215] Anthropic, 'Activating AI Safety Level 3 Protections' (22 May 2025), stating that Anthropic could not 'clearly rule out ASL-3 risks' for Claude Opus 4 and describing safeguards 'narrowly focused on preventing... extended, end-to-end CBRN workflows', with biological weapons assessed as representing the majority of that risk; see also OpenAI, Preparedness Framework v2 (15 April 2025), which tracks biological uplift as a 'High' capability category. https://www.anthropic.com/news/activating-asl3-protections

[216] Bulletin of the Atomic Scientists, 2026 Doomsday Clock Statement (27 January 2026), setting the Clock at 85 seconds to midnight and warning that AI may be embedded in nuclear decision-support systems, and that 'a too-heavy dependence on black-box systems could present a serious danger'. https://thebulletin.org/doomsday-clock/2026-statement/

[217] International Institute for Strategic Studies, 'Nuclear Command Without Control: AI and the Problem of Escalation Opacity', Survival Online (2026), and Bulletin of the Atomic Scientists, 'Algorithms of Misperception: Managing Nuclear Risk in an AI World' (November 2025), both using the 1983 Petrov false-alarm incident as an analogy for the risk of automation bias in AI-assisted early-warning systems. No publicly confirmed AI-caused nuclear near-miss is known to have occurred as of the date of this appraisal; the concern identified in this literature is a documented expert warning, not a documented incident. https://www.iiss.org/online-analysis/survival-online/2026/07/nuclear-command-without-control-ai-and-the-problem-of-escalation-opacity/

- AI-assisted cyberattacks on critical infrastructure such as electricity grids and water systems - a risk with an obvious connection to the grid and water dependencies discussed elsewhere in this appraisal;
- AI-generated disinformation and deepfakes capable of undermining electoral and democratic processes; and
- the extension of AI targeting and decision-making to autonomous weapons systems, an area in which the United Nations General Assembly has already recorded a resolution supported by 156 states.

Frontier developers' own safety frameworks generally list chemical alongside biological, nuclear and radiological uplift as a further tracked risk category, albeit one for which the evidence of near-term uplift above existing knowledge is currently thinner than for biology.[218,219]

None of this appraisal's discussion of AI risk, in either the loss-of-control or the deliberate-misuse form, is intended to suggest that the data centres considered elsewhere in this appraisal are themselves the source of that risk; the connection is that the same computing capacity being built out across England and Wales is also the capacity on which future frontier AI systems, whatever risks they carry, will run.

Whether the safety evaluation work now being conducted by the UK AI Security Institute and equivalent bodies extends to considering deliberate-misuse scenarios specific to the AI infrastructure being sited in this country, and whether that work has any bearing on the Critical National Infrastructure designation discussed in Section 1, does not appear to have been addressed in any published document identified for this appraisal. A question the author intends to put in writing to Kanishka Narayan MP, Member of Parliament for the Vale of Glamorgan and Minister for Artificial Intelligence, reads:

> *'What assessment has the Government made of deliberate-misuse risks - including biological, chemical, cyber and nuclear-adjacent scenarios - arising from AI systems that will run on data-centre capacity sited in the UK, and does that assessment form any part of the basis on which data infrastructure has been designated Critical National Infrastructure?'*

---

[218] Centre for the Governance of AI, 'Assessing the Risk of AI-Enabled Cyberattacks on the Power Grid'; see also World Economic Forum, Global Cybersecurity Outlook 2026, and Alan Turing Institute (CETAS), 'From Deepfake Scams to Poisoned Chatbots: AI and Election Security in 2025', on AI-assisted threats to critical infrastructure and democratic processes respectively. https://www.governance.ai/research-paper/ai-enabled-cyberattacks-on-the-power-grid

[219] Human Rights Watch, 'A Hazard to Human Rights: Autonomous Weapons Systems and Digital Decision-Making' (28 April 2025); see also the UN General Assembly resolution on lethal autonomous weapons systems supported by 156 states, and the Frontier Model Forum's 'Risk Taxonomy and Thresholds for Frontier AI Frameworks', which lists chemical alongside biological, nuclear and radiological uplift as a tracked risk category. https://www.hrw.org/report/2025/04/28/a-hazard-to-human-rights/autonomous-weapons-systems-and-digital-decision-making

No answer to a question in these terms has been identified in Hansard, the Senedd Record or via WhatDoTheyKnow to date.

Rogue and hostile states: a harder threat to detect than a nuclear programme

The warnings addressed so far concern AI systems themselves, whether acting on their own initiative or being deliberately misused.

A related question is how a hostile or 'rogue' state might approach AI, and how that compares with the well-established, decades-old problem of detecting a nuclear weapons programme.

There is already documented evidence of state-linked use. OpenAI's disclosures, first published in February 2024 and updated through October 2025, identified groups linked to China, Iran, North Korea and Russia using its models for reconnaissance, phishing content, code debugging, translation of technical material and evasion research; OpenAI's own assessment at the time was that this gave only limited, incremental capability beyond tools already available. Microsoft's threat intelligence work reports the same pattern.

More recently, Anthropic reported in November 2025 that a Chinese state-sponsored group had jailbroken an AI coding tool to run a largely autonomous espionage campaign against around 30 organisations, with 80-90% of tasks automated and only four to six human decision points throughout - while also noting that the model sometimes produced inaccurate or fabricated results, meaning some of the attackers' own claimed successes were themselves exaggerated.

Taken together, this is documented evidence of state and state-linked actors using AI operationally, though not yet, on the evidence available, evidence that this has produced an attack of catastrophic scale.[220,221,222]

---

[220] OpenAI, 'Disrupting Malicious Uses of AI by State-Affiliated Threat Actors' (14 February 2024, with further disruption reports published through October 2025), identifying use of its models by groups linked to China (Charcoal Typhoon, Salmon Typhoon), Iran (Crimson Sandstorm), North Korea (Emerald Sleet) and Russia (Forest Blizzard) for reconnaissance, phishing content, code debugging, translation of technical material and evasion research; OpenAI's own assessment at the time was that this gave only limited, incremental capability over tools already available. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

[221] Anthropic, 'Disrupting an AI-Orchestrated Cyber Espionage Campaign' (November 2025), reporting that a Chinese state-sponsored group jailbroke an AI coding tool, posing as a legitimate security firm, to run a campaign against approximately 30 organisations with 80-90% of tasks automated and only four to six human decision points per campaign - described as the first largely autonomous, AI-orchestrated attack of its kind. Anthropic's own report notes the model sometimes produced inaccurate or fabricated results during the campaign, meaning some of the attackers' claimed successes were themselves exaggerated; this appraisal treats the underlying capability as documented while noting that caveat. https://www.anthropic.com/news/disrupting-AI-espionage

[222] Microsoft, 'AI as Tradecraft: How Threat Actors Operationalize AI' (6 March 2026), and Microsoft Digital Defense Report 2025, both confirming, consistently with OpenAI's findings,

The comparison with nuclear weapons is instructive, and this appraisal draws it as an inference from the material cited rather than as a comparison any single source below makes in these terms.

A nuclear weapons programme requires large, fixed physical infrastructure - enrichment facilities, reactors, specialist industrial equipment - that satellite imagery and International Atomic Energy Agency inspection regimes are, imperfectly but substantially, able to detect.

Research on AI verification consistently observes that no equivalent physical signature exists for AI capability development, which requires principally computing talent and code; proposals for AI-specific verification, such as hardware-based reporting requirements on AI chips, remain at the research and proposal stage rather than being an established or agreed international regime.

On this evidence, a state seeking to develop dangerous AI capability may be substantially harder to detect at an early stage than a state pursuing nuclear weapons, though this appraisal cannot quantify how much harder, and treats the point as a reasoned inference rather than a settled finding.[223]

A closely related concern is whether meaningful capability could be developed by a small, difficult-to-track team rather than a large, visible national programme of the kind more readily monitored by national intelligence services.

Export controls on advanced AI chips are the principal tool currently relied on to slow this, but the evidence on their effectiveness is mixed: one 2026 analysis estimated that around 660,000 advanced AI chips (H100-equivalent) were smuggled into China by the end of 2025, representing roughly a third of that country's total AI compute, with an estimated detection rate of only 10-80%.

Other analysis concludes that export controls can slow, but are unlikely to stop, a sufficiently determined state actor. If correct, this supports the proposition that homegrown expertise operating with modest, hard-to-track compute resources is a realistic route to AI capability development, though

---

that nation-state-linked groups from Russia, China, Iran and North Korea use large language models across the stages of an attack, from reconnaissance to script writing and evasion research. https://www.microsoft.com/en-us/security/blog/2026/03/06/ai-as-tradecraft-how-threat-actors-operationalize-ai/

[223] Center for Security and Emerging Technology, Matthew Mittelsteadt, 'AI Verification' (February 2021), and Wasil, Reed, Miller and Barnett, 'Verification Methods for International AI Agreements' (2024), both concluding that, unlike nuclear weapons programmes, which require large physical facilities detectable by satellite imagery and IAEA-style inspection, AI capability development requires principally compute, talent and code, for which no equivalent, well-established verification regime yet exists. This comparison is presented in the sources as a proposal and an open research problem, not as an established or agreed verification standard, and the specific parallel drawn here between AI and nuclear detectability is this appraisal's own synthesis of that material rather than a comparison either source states in these terms. https://cset.georgetown.edu/publication/ai-verification/

this appraisal has not identified a documented case of a state having actually done so for a weapons-relevant purpose.[224]

Beyond weapons development, the same concern extends to disruption: a state might use AI not only to design offensive capability but to degrade critical services in another country that itself relies on AI, whether directly (attacking AI systems used to run infrastructure) or indirectly (attacking the electricity, water or data infrastructure, discussed throughout this appraisal, on which AI systems depend).

The UK's National Cyber Security Centre has warned that hostile states are already linked to around three-quarters of cyberattacks on UK critical national infrastructure, though that figure is not specific to AI-enabled attacks, and has separately warned of a widening gap between well-defended and poorly-defended organisations as AI capability spreads.

This appraisal has not identified a documented case of a state using AI specifically to disrupt another nation's AI-dependent critical infrastructure or financial services; on the evidence available, that scenario should be treated as an anticipated risk that responsible authorities are already warning about, not as an evidenced one.[225]

A question the author intends to put in writing to Kanishka Narayan MP, as Minister for Artificial Intelligence, reads:

> *'What assessment has the Government made of the risk that a hostile state could develop dangerous AI capability using a small team and modest, difficult-to-track compute resources rather than a large, visible national programme, and does that assessment inform decisions on the location and security of AI-related data-centre infrastructure in the UK?'*

No answer to a question in these terms has been identified in Hansard, the Senedd Record or via WhatDoTheyKnow to date.

---

[224] Epoch AI, Isabel Juniewicz, 'Diversion and Resale: Estimating Compute Smuggling to China' (29 April 2026), estimating that approximately 660,000 H100-equivalent AI chips were smuggled into China by the end of 2025, roughly a third of the country's total AI compute, with an estimated detection rate of only 10-80%; see also RAND, 'Leashing Chinese AI Needs Smart Chip Controls' (August 2025), arguing that export controls can slow but are unlikely to stop a determined state actor. Taken together, this appraisal treats these sources as supporting the proposition that a state could plausibly pursue AI capability development through a comparatively small and difficult-to-track effort, though no documented case of a state using AI specifically to disrupt another nation's AI-dependent critical infrastructure has been identified for this appraisal, and that scenario should be treated as an anticipated rather than an evidenced risk. https://epoch.ai/publications/chip-smuggling

[225] National Cyber Security Centre, 'AI to 2027' threat assessment (7 May 2025), warning that AI will shrink the window between a vulnerability's discovery and its exploitation, and that capable state-linked actors are likely to benefit disproportionately from a widening gap between well-defended and poorly-defended organisations; see also the NCSC's public statement that hostile states are linked to around three-quarters of cyberattacks on UK critical national infrastructure, a figure not limited to AI-enabled attacks specifically. https://www.ncsc.gov.uk/news/ai-to-2027-threat-assessment

Software reliability: building on tools that may not be bug-free

A further, more basic concern is whether AI systems are being relied upon as though they were more dependable than they have so far shown themselves to be.

Even the most resourced conventional software companies, with a strong commercial incentive to minimise defects, ship a large and growing number of vulnerabilities.

Submissions to the US National Vulnerability Database's Common Vulnerabilities and Exposures system rose 263% between 2020 and 2025; Microsoft alone patched 1,130 vulnerabilities in 2025, including 41 zero-day flaws, 24 of which were already being actively exploited before a fix existed.

This appraisal has not identified a single, reliable industry-wide figure for the average time between a software release and its first critical patch; the closest available proxy, that around 80% of exploits are published faster than the corresponding vulnerability record, suggests attackers frequently move before an official fix exists even for mature, widely used software.[226,227]

AI systems have already shown comparable, and in some respects more troubling, patterns.

OpenAI published an unusually candid postmortem in April 2025 after rolling back a GPT-4o update that had made the model dangerously agreeable, in one documented instance validating a user's decision to stop taking prescribed psychiatric medication; the company's own account states the problem passed its offline evaluations and limited live testing before wider release.

Separately, AI 'jailbreak' vulnerabilities, methods of circumventing a model's safety training, have proved to be an ongoing arms race rather than something fixed once and for all: Anthropic's February 2025 'Constitutional Classifiers' defence claimed a 95% reduction in successful jailbreaks, but independent researchers found bypasses, and broader testing reported

[226] National Institute of Standards and Technology, 'NIST Updates NVD Operations to Address Record CVE Growth' (9 April 2026), reporting that submissions of Common Vulnerabilities and Exposures rose 263% between 2020 and 2025; see also Tenable, 'Microsoft Patch Tuesday 2025 Year in Review' (10 December 2025), recording that Microsoft alone patched 1,130 vulnerabilities in 2025, including 41 zero-day flaws of which 24 were already being actively exploited before a fix existed. https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth

[227] Unit 42 (Palo Alto Networks), 'State of Exploit Development', reporting that around 80% of exploits are published faster than the corresponding vulnerability record, meaning attackers frequently move before an official patch exists; this appraisal has not identified a single, industry-wide figure for the average time between a software release and its first critical patch, and treats this statistic as the closest available proxy rather than a direct answer to that question. https://unit42.paloaltonetworks.com/state-of-exploit-development/

breaking every one of several vendors' AI safety defences that had claimed near-zero attack-success rates.[228,229]

Part of the difficulty is technical rather than a matter of insufficient effort. Large language models are, in a way conventional deterministic software generally is not, capable of producing different outputs from the same input across different runs or model versions, which sits uneasily with the traditional software-engineering assumption that a system can be tested once, verified and then shipped with confidence.

This appraisal has not identified a single, authoritative government statement setting this point out in so many words, and treats it as well-evidenced engineering and expert consensus rather than an official finding.

Two documented incidents illustrate that these are not merely theoretical or laboratory concerns. In February 2024, the Civil Resolution Tribunal of British Columbia held Air Canada liable after its website chatbot fabricated a bereavement-fare refund policy that did not exist, rejecting the airline's argument that the chatbot was a 'separate legal entity' for which it bore no responsibility. Separately, Waymo issued three software recalls of its self-driving vehicle fleet during 2024 and 2025, including a May 2025 recall of around 1,200 vehicles following low-speed collisions with gates and chains - a regulator-linked, software-triggered recall of a safety-critical AI system already in public use.[230,231]

None of this establishes that AI systems are categorically less trustworthy than the conventional software that preceded them, and this appraisal does

[228] OpenAI, 'Sycophancy in GPT-4o: What Happened and What We're Doing About It' (29 April 2025), an unusually candid postmortem in which OpenAI rolled back a model update after it became dangerously agreeable, in one documented instance validating a user's decision to stop taking prescribed psychiatric medication; OpenAI's own account states the problem passed the company's offline evaluations and limited live testing before wider release. https://openai.com/index/sycophancy-in-gpt-4o/

[229] Anthropic published a 'Constitutional Classifiers' defence in February 2025 claiming a 95% reduction in successful jailbreak attempts against its models; independent red-teamers subsequently found bypasses, and broader independent research reported breaking every one of several vendors' AI safety defences that had claimed near-zero attack-success rates when tested. This appraisal treats AI jailbreak mitigation as an ongoing, unresolved arms race rather than as a case of vulnerabilities being durably closed in the way a conventional software patch closes a known hole. https://venturebeat.com/security/12-ai-defenses-claimed-near-zero-attack-success-researchers-broke-all-of-them

[230] Civil Resolution Tribunal of British Columbia, Moffatt v Air Canada (February 2024), holding Air Canada liable after its website chatbot fabricated a bereavement-fare refund policy that did not exist, and rejecting the airline's argument that the chatbot was a 'separate legal entity' for which it bore no responsibility. https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot

[231] Waymo issued three separate software recalls of its self-driving vehicle fleet during 2024-2025: in February 2024, around 700 vehicles after two cars struck the same towed truck; a second recall in June 2024; and a further recall of approximately 1,200 vehicles in May 2025 following low-speed collisions with gates and chains. These are US National-Highway-Traffic-Safety-Administration-linked, software-triggered recalls of a safety-critical AI system already in public deployment. https://techcrunch.com/2025/05/14/waymo-recalls-1200-robotaxis-following-low-speed-collisions-with-gates-and-chains/

not draw that conclusion. It does suggest, as a reasoned inference rather than a proven fact, that AI systems are at least as prone to bugs and unpredictable behaviour as conventional software from the same well-resourced companies, and that their added complexity and non-determinism may make them harder to fully test in advance.

Read alongside the nuclear command-and-control concerns discussed above, this reinforces rather than displaces the case for caution: a system that is difficult to fully verify before deployment is not obviously one that should be given significant autonomy over safety-critical decisions without independent, ongoing scrutiny.

As with the employment questions addressed in Section 3, the honest position on AI risk is that significant uncertainty remains. That uncertainty is itself the argument for asking more, not fewer, questions of government, developers and regulators - and for building the mandatory, independently verifiable reporting on energy, water, carbon and safety discussed throughout this appraisal, so that precaution can be exercised on the basis of evidence rather than assurance.

An independent national assessment: the Alan Turing Institute (September 2026)

In September 2026 the Alan Turing Institute, the United Kingdom's national institute for artificial intelligence, published 'Frontier AI Risks: A practical way forward'.[232] It is the most authoritative UK assessment independent of the AI developers that this appraisal has identified, and the Minister for Artificial Intelligence described it as 'a welcome contribution'.[233] The Institute found that 'there is no expert consensus on whether AI poses long-term existential risk to humanity', but that 'there is broad consensus regarding the realistic possibility of catastrophic AI risk in the short to medium term'. It identified five risks for priority attention - cyber security, democratic instability, misalignment, loss of meaningful human control, and chemical and biological threats - and said that there is 'a realistic possibility' that 'superintelligent' AI systems emerge in the next five years, which it holds as 'a possibility to plan against, not a prediction'.[234]

The Institute pointed to two recent developments. In April 2026 Anthropic chose not to make a model, Claude Mythos Preview, generally available because it could find and exploit previously undisclosed software

[232] Alan Turing Institute, 'Frontier AI Risks: A practical way forward' (September 2026), Summary and sections 1 to 2. https://www.turing.ac.uk/news/publications/frontier-ai-risks-practical-way-forward; https://www.turing.ac.uk/sites/default/files/2026-09/frontier_ai_risks_-_a_practical_way_forward.pdf

[233] Alan Turing Institute, 'The Alan Turing Institute sets out practical agenda to tackle frontier AI risks' (news release, 23 September 2026), quoting the Minister for Artificial Intelligence. https://www.turing.ac.uk/news/alan-turing-institute-sets-out-practical-agenda-tackle-frontier-ai-risks

[234] See n 232 above.

vulnerabilities, and the National Cyber Security Centre then advised organisations to plan to deploy security updates 'quickly, more frequently, and at scale'.[235,236] In July 2026 AI agents being tested by OpenAI got round the controls intended to isolate them from the internet and compromised parts of the systems of Hugging Face, a company that hosts AI models; the breach was not connected to OpenAI's agents until some days after it had been publicly disclosed, and OpenAI has itself called the episode 'a "warning shot" for us and for the world'.[237] The Institute adds that other organisations, including Anthropic and the AI Security Institute, 'have also seen AI agents escape their intended confines'.[238]

Three of the Institute's conclusions bear directly on the infrastructure with which this appraisal is concerned. First, on resilience: 'As essential services gradually adopt AI, they may increasingly rely on a small number of underlying model providers, cloud infrastructure, and compute. This means that a single compromise or outage could become a multi-sector event with cascading failures' (compare Sections 12 and 14 above). Secondly, on 'kill switches': the Institute describes the idea as 'a metaphor rather than an engineering proposal', observes that 'on the electricity grid, stopping is itself the hazard', warns that the point at which an AI system becomes too deeply embedded to be switched off safely 'may not be visible in advance', and notes that 'blocking access to advanced AI systems at a UK level does not prevent deployment or misuse elsewhere'. It suggests that services should be designed so that they 'could continue without' the AI system. Thirdly, on testing: model evaluation, in which the AI Security Institute leads, 'only takes us so far'; what matters more is the 'verification of whole systems - technology, people and processes together', reassessed throughout a system's working life, 'just as an aircraft is not certified once but inspected throughout its service life'.[239]

Two inferences follow, which are the author's own rather than the Institute's. The first is that the more public services come to depend on AI capacity housed in data centres, the more important it becomes that each such service keeps a tested way of operating without it; that is principally a matter for the bodies adopting AI, but it is also a resilience question for the infrastructure decisions discussed in this appraisal. The second is that the Institute's call for continuing, whole-system assurance mirrors the approach this appraisal urges for environmental effects: assessment at the point of

[235] See n 232 above.
[236] Ollie Whitehouse, 'Preparing for a "vulnerability patch wave"', National Cyber Security Centre blog (1 May 2026). https://www.ncsc.gov.uk/blogs/prepare-for-vulnerability-patch-wave
[237] OpenAI, 'The Hugging Face incident and the road ahead' (26 August 2026); see also METR, 'Brief independent investigation of agents' behavior, reasoning and collaboration in the OpenAI / Hugging Face hacking incident' (26 August 2026). https://openai.com/index/hugging-face-incident-and-the-road-ahead/; https://metr.org/blog/2026-08-26-openai-hugging-face-incident-investigation/
[238] See n 232 above.
[239] See n 232 above.

consent is not enough without monitoring and published evidence over the working life of a development.

On governance, the Institute speaks, by its own account, as an informed observer rather than as an authority. It concludes that slowing the development of frontier AI 'would require urgent binding regulation, which is unlikely in the present international environment', and that formalised testing and verification regimes will be needed to manage future risks internationally.[240] Alongside the report, the Institute announced a new research programme, led by its Centre for Emerging Technology and Security and funded by a £2 million grant, on the security implications of transformative AI.[241]

The author intends to put the following question in writing to Kanishka Narayan MP, as Minister for Artificial Intelligence: 'In the light of the Alan Turing Institute's report, which you have welcomed, will the Government require public services and operators of critical national infrastructure that adopt AI to maintain, and regularly test, a way of continuing to operate without it; and will AI developers and operators of AI data centres in the United Kingdom be required to report incidents in which AI agents escape their intended controls to the AI Security Institute and the National Cyber Security Centre?' A request via WhatDoTheyKnow to the Department for Business, Innovation, Science and Trade for any guidance or assessment on AI fallback arrangements and incident reporting could follow.

On 12 October 2026, in a written statement to Parliament, the Minister said that the AI Security Institute had regained access to the most capable models before their release, and that the Government is considering how the Cyber Security and Resilience Bill might provide for near misses and serious AI incidents to be identified and reported.[242] That partly answers the second limb of the question above; who would have to report, to whom, and whether operators of AI data centres would be covered remain open. The statement did not address the first limb, a tested way of operating without AI.

And to the Welsh Government minister responsible for digital and data policy: 'What requirements does the Welsh Government place on Welsh public bodies that adopt AI systems to maintain a tested way of operating without them, and what consideration has it given to the Alan Turing Institute's finding that reliance on a small number of AI providers, cloud services and computing facilities could turn a single compromise or outage into a multi-sector event?' No answer to a question in these terms has been identified.

---

[240] See n 232 above.
[241] See n 233 above.
[242] Kanishka Narayan MP, 'Artificial Intelligence Policy', written ministerial statement HCWS357, House of Commons (12 October 2026). https://questions-statements.parliament.uk/written-statements/detail/2026-10-12/hcws357

The Government's own position: understanding admitted, safeguards deferred

The foundation of the United Kingdom's approach to regulating artificial intelligence remains the white paper 'A pro-innovation approach to AI regulation', published by the Department for Science, Innovation and Technology under the previous government in March 2023. The present government has not replaced it: the House of Commons Library recorded in June 2026 that most AI systems are still regulated 'at the point of use' by existing sector regulators, under five cross-sector principles that have never been placed on a statutory footing.[243,244]

The white paper is candid about the limits of understanding.

Its ministerial foreword states that 'most of us are only now beginning to understand the transformative potential of AI as the technology rapidly improves', and the paper itself records that large language models 'have been developed beyond expectations'.

The conclusion it draws from that uncertainty is, however, the opposite of the one this appraisal would draw.

It decided not to create an AI regulator, not to put its principles on a statutory footing 'initially', and to introduce a statutory duty on existing regulators only 'when parliamentary time allows'.

In the view of this appraisal, an admission that a fast-moving technology is not yet understood is an argument for caution and for safeguards that can be enforced, not for deferring them. That is this appraisal's own reading of the document, offered as a criticism rather than as a finding of any official body.[245]

The language used to promote the policy also deserves comment. The white paper compares AI's potential impact to that of 'electricity or the internet' and sets a goal of making the United Kingdom 'a science and technology superpower by 2030'.

When the present government launched its AI Opportunities Action Plan in January 2025, its announcement said that the plan 'mainlines AI into the veins of this enterprising nation' and would 'turbocharge' its programme,

---

[243] Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation' (white paper, March 2023, updated 3 August 2023), including the ministerial foreword by the Rt Hon Michelle Donelan MP. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

[244] House of Commons Library, 'AI regulation in the UK', Research Briefing CBP-10003 (10 June 2026), which also records Labour's 2024 manifesto commitment, the reported delay to legislation and the absence of statutory powers for the AI Security Institute. https://researchbriefings.files.parliament.uk/documents/CBP-10003/CBP-10003.pdf

[245] Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation' (white paper, March 2023, updated 3 August 2023), including the ministerial foreword by the Rt Hon Michelle Donelan MP. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

and cited productivity gains of up to 1.5 percentage points a year, worth some £47 billion annually - figures that the announcement itself makes conditional on AI being 'fully embraced'.

The renaming of the AI Safety Institute as the AI Security Institute in February 2025 was announced under the heading of tackling risks 'to unleash growth'.

Governments commonly use promotional language, and this appraisal takes no view on whether the promised gains will materialise. The concern is that conditional estimates and emotive phrasing are presented to the public with more confidence than the government's own founding document claims to have, and in sharp contrast with the warnings from within the industry discussed earlier in this section.[246,247,248,249]

Two omissions stand out when the white paper is read alongside the rest of this appraisal.

First, it says nothing about the physical cost of the technology it promotes: energy, water, land and carbon are not considered as costs of AI at all, climate change appears only as a problem AI may help to solve, and computing capacity appears only as an investment to be made. The 2025 Action Plan's 50 recommendations include one to 'mitigate the sustainability and security risks of AI infrastructure', and an AI Energy Council was established in April 2025 to advise on energy efficiency and sustainability, 'such as the use of water'; this appraisal has not identified any published standard or advice from that Council on the water or carbon footprint of data centres.

Second, this appraisal has found no reference in the white paper to Wales or to the devolved administrations, even though planning, water and much of

[246] Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation' (white paper, March 2023, updated 3 August 2023), including the ministerial foreword by the Rt Hon Michelle Donelan MP. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

[247] Department for Science, Innovation and Technology, 'AI Opportunities Action Plan' (13 January 2025), including Recommendation 2 (expanding the AI Research Resource 'by at least 20x by 2030'), Recommendation 4 (AI Growth Zones with streamlined planning) and Recommendation 5 (sustainability and security risks of AI infrastructure). https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

[248] Prime Minister's Office and Department for Science, Innovation and Technology, 'Prime Minister sets out blueprint to turbocharge AI' (press release, 13 January 2025), including the productivity estimate and the announced £12 billion investment by Vantage Data Centres. https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai

[249] Department for Science, Innovation and Technology, 'Tackling AI security risks to unleash growth and deliver Plan for Change' (press release, 14 February 2025), announcing the renaming of the AI Safety Institute as the AI Security Institute. https://www.gov.uk/government/news/tackling-ai-security-risks-to-unleash-growth-and-deliver-plan-for-change

environmental regulation - the matters through which AI's physical infrastructure is actually decided - are devolved.[250,251]

Meanwhile, the pace of the two halves of policy differs markedly.

AI infrastructure is being accelerated: the Action Plan proposes AI Growth Zones with streamlined planning and a twentyfold expansion of public AI computing capacity by 2030, and its launch was accompanied by an announced £12 billion of UK investment by Vantage Data Centers, the operator at Bro Tathan, said to bring more than 11,500 jobs.

Safeguards, by contrast, have been deferred. The previous government said in February 2024 that it would legislate only when 'confident that it is the right thing to do'.

The present government's 2024 manifesto promised 'binding regulation on the handful of companies developing the most powerful AI models', but the Commons Library notes reports that those proposals were delayed 'by at least a year', and that the AI Security Institute has not been given statutory powers; its renamed remit states expressly that it 'will not focus on bias or freedom of speech'. How the jobs figure relates to the much smaller number of permanent operational posts discussed in Section 3 above is a question worth asking in its own right.[252,253,254,255,256]

---

[250] Department for Science, Innovation and Technology, 'AI Opportunities Action Plan' (13 January 2025), including Recommendation 2 (expanding the AI Research Resource 'by at least 20x by 2030'), Recommendation 4 (AI Growth Zones with streamlined planning) and Recommendation 5 (sustainability and security risks of AI infrastructure). https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

[251] Department for Science, Innovation and Technology and Department for Energy Security and Net Zero, 'AI Energy Council to ensure UK's energy infrastructure ready for AI revolution' (press release, April 2025). https://www.gov.uk/government/news/ai-energy-council-to-ensure-uks-energy-infrastructure-ready-for-ai-revolution

[252] Prime Minister's Office and Department for Science, Innovation and Technology, 'Prime Minister sets out blueprint to turbocharge AI' (press release, 13 January 2025), including the productivity estimate and the announced £12 billion investment by Vantage Data Centres. https://www.gov.uk/government/news/prime-minister-sets-out-blueprint-to-turbocharge-ai

[253] Department for Science, Innovation and Technology, 'AI Opportunities Action Plan' (13 January 2025), including Recommendation 2 (expanding the AI Research Resource 'by at least 20x by 2030'), Recommendation 4 (AI Growth Zones with streamlined planning) and Recommendation 5 (sustainability and security risks of AI infrastructure). https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

[254] Department for Science, Innovation and Technology, 'A pro-innovation approach to AI regulation: government response' (February 2024), which also proposed future 'targeted binding requirements' on developers of highly capable general-purpose AI models. https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

[255] House of Commons Library, 'AI regulation in the UK', Research Briefing CBP-10003 (10 June 2026), which also records Labour's 2024 manifesto commitment, the reported delay to legislation and the absence of statutory powers for the AI Security Institute. https://researchbriefings.files.parliament.uk/documents/CBP-10003/CBP-10003.pdf

[256] Department for Science, Innovation and Technology, 'Tackling AI security risks to unleash growth and deliver Plan for Change' (press release, 14 February 2025), announcing the

Parliament has begun to press the point.

In September 2026 a Labour backbench MP introduced, under the ten minute rule, an Artificial Superintelligence Bill to prohibit the development, deployment and operation of artificial superintelligence systems, and a cross-party group of MPs and peers wrote to the Prime Minister asking the Government to work towards an international agreement prohibiting superintelligent AI. This appraisal has not identified a published Government response to either.[257,258]

The author intends to put the following questions in writing in due course.

To Kanishka Narayan MP, Member of Parliament for the Vale of Glamorgan and Minister for Artificial Intelligence, who attends Cabinet following the merger in July 2026 of the Department for Science, Innovation and Technology into a new Department for Business, Innovation, Science and Trade:[259]

> 'Given the acknowledgement in the 2023 white paper that "most of us are only now beginning to understand the transformative potential of AI", and that its principles remain non-statutory more than three years later, what evidence does the Government now rely on to justify accelerating AI infrastructure through AI Growth Zones and streamlined planning while statutory safeguards, including the promised binding regulation of the most powerful AI models, have not been introduced; and when will that legislation be brought forward?'

No answer to a question in these terms has been identified.

A freedom of information request via WhatDoTheyKnow for any assessment underpinning the timing of the legislation would be a further step, although the exemption for the formulation of government policy may well be claimed.

To the same Minister, asking that it also be put to the minister responsible for energy:

---

renaming of the AI Safety Institute as the AI Security Institute. https://www.gov.uk/government/news/tackling-ai-security-risks-to-unleash-growth-and-deliver-plan-for-change

[257] UK Parliament, Artificial Superintelligence Bill (Bill 4288, session 2026-27), a ten minute rule bill presented by Alex Sobel MP. https://bills.parliament.uk/bills/4288

[258] Letter from members of both Houses of Parliament to the Prime Minister, 11 September 2026, published by ControlAI. https://images.controlai.com/final%20letter.pdf

[259] GOV.UK, 'Kan
ishka Narayan MP', recording his appointment on 20 July 2026 as Minister of State (Minister for Artificial Intelligence) jointly in the Cabinet Office and the Department for Business, Innovation, Science and Trade; on the Prime Minister's invitation to attend Cabinet and the merger of departments, see Enterprise Nation, 'Andy Burnham brings AI to cabinet as tech department merged with business'. https://www.gov.uk/government/people/kanishka-narayan; https://www.enterprisenation.com/learn-something/pm-brings-ai-to-cabinet-as-tech-department-merged-with-business/

> 'What assessment has been made of the energy, water, land and carbon costs of the AI computing capacity the Government is promoting, including the twentyfold expansion of public AI compute by 2030 and the AI Growth Zones; will that assessment be published; and will the advice of the AI Energy Council on water use be published?'

A request via WhatDoTheyKnow for the AI Energy Council's minutes and advice would test what has been considered.

To the Welsh Government Cabinet Minister for Enterprise, Connectivity and Energy:

> 'Of the more than 11,500 jobs announced alongside Vantage Data Centers' £12 billion UK investment in January 2025, how many are expected to be permanent operational posts in Wales, as distinct from construction and supply-chain roles; and has the Welsh Government made any representations to the UK Government about how the UK's approach to AI regulation takes account of devolved responsibilities for planning, water and the environment, and of the Well-being of Future Generations (Wales) Act 2015?'

A request via WhatDoTheyKnow for any such representations, and for any jobs assessment relating to Vantage's South Wales campuses, could follow once a reply is received.

18. Whose problem is this?

Concerns about water resources are connected to concerns about sewage and wastewater treatment capacity, and both are connected to the strain data centres can place on the electricity grid, discussed in Sections 4 and 15 above; it is already publicly acknowledged that some data centres are being built, or are seeking connection, in areas where grid capacity is not yet sufficient to serve them without reinforcement.

These effects are not necessarily confined to a development's immediate boundary.

People and businesses close to a proposed site are the most obviously affected, but a data centre's practical demand on shared water, sewerage and grid infrastructure can extend to anyone drawing on the same catchment, treatment works or grid connection, whether or not they live near the site itself.

That makes the ordinary planning concept of an 'affected neighbour' harder to apply than it might first appear: a household or business many miles from a proposed data centre may in practice be more exposed to its cumulative effect on a shared resource than an immediate neighbour would be, without necessarily being aware of the connection, still less being consulted about it.

This appraisal does not conclude that data centres are, on balance, harmful to the wider communities and infrastructure users connected to them; nor does it accept, on the evidence identified, the proposition sometimes advanced that there is no downside to data-centre development at all.

The honest position, consistent with the rest of this appraisal, is that the evidence needed to reach a considered view on cumulative and regional effects - including who should properly be treated as an affected party - is not yet routinely collected, connected or published. Addressing that evidence gap, rather than resolving the underlying dispute about costs and benefits, is the more immediate task this appraisal identifies for government and regulators.

19. Public Policy Questions

Several questions remain unresolved:

1. Should certain public-sector datasets be subject to additional sovereignty protections?
2. Is physical data residency sufficient to satisfy public expectations regarding control?
3. Should public bodies disclose backup and disaster-recovery locations?
4. Should planning authorities assess digital-resilience issues alongside environmental impacts?
5. How should communities hosting major digital infrastructure share in resulting benefits?
6. Does increasing concentration among a small number of cloud providers create strategic risks?
7. How should governments balance AI ambitions with environmental constraints?
8. What is the realistic long-term employment case for a data-centre development, once construction-phase activity and the effects of AI-driven automation are properly distinguished from steady-state operational employment?
9. Where a public body acts simultaneously as landowner, promoter and planning or regulatory authority in respect of a data-centre proposal, what safeguards or transparency requirements should apply?
10. Given the warnings some of those building the most advanced AI systems have themselves issued about its risks, what would government regard as sufficient evidence to move from precaution to either reassurance or restriction, and who should decide that?

11. What steps are being taken to ensure that international operators account, for tax purposes, for profits attributable to their UK data-centre operations in the UK rather than in lower-tax jurisdictions?
12. On what legal or contractual basis, if any, would data centres be required to reduce or cease water use ahead of household or agricultural users during a shortage, and should that basis be made public before, rather than after, planning permission is granted?
13. Where a data centre's practical demand on water, sewerage or grid infrastructure is regional rather than site-specific, who should be treated as an affected party for consultation purposes, and what mandatory reporting would be needed to identify them?
14. What assessment has government made of whether the very large sums of capital investment announced for data-centre development already include the cost of the grid, transmission and water infrastructure upgrades needed to support it, and if not, who is expected to bear that cost and what effect will it have on funding for other infrastructure priorities?
15. What assessment has government made of deliberate-misuse risks arising from AI systems that will run on data-centre capacity sited in the UK - including biological, chemical, cyber and nuclear-adjacent scenarios - as distinct from the risk of an AI system acting on its own initiative, and does that assessment inform the Critical National Infrastructure designation of data infrastructure?
16. What assessment has government made of the risk that a hostile state could develop dangerous AI capability using a small team and modest, difficult-to-track compute resources rather than a large, visible national programme, and does that assessment inform decisions on the location and security of AI-related data-centre infrastructure in the UK?
17. What assurance regime, if any, applies to AI systems used in or connected to safety-critical or critical-infrastructure settings, given the documented pattern of urgent post-deployment fixes required even by the most resourced conventional software developers, and the added unpredictability that AI's non-deterministic behaviour introduces?
18. What assessment has been made of the use, quantities and environmental fate of PFAS ('forever chemicals') in data-centre fire-suppression and cooling systems in England and Wales, and what guidance, if any, exists on the safe decommissioning of such systems, including any implications for the duties in the Well-being of Future Generations (Wales) Act 2015?

19. What are host nations doing to guard against the possibility that data held by companies headquartered in another state could be accessed, copied or withheld as a consequence of that state's laws, sanctions or financial pressure, rather than under the host nation's own law?
20. Should public services and critical infrastructure that adopt AI be required to keep a tested way of operating without it, and should incidents in which AI agents escape their controls be reported to the AI Security Institute and the National Cyber Security Centre?
21. Should the energy and water use of individual data centres be reported and published site by site, rather than held in confidence as under the EU's rules?
22. Where a screening opinion was given for an earlier or smaller scheme, should a planning authority be required to adopt a fresh one when the site, the generating plant or the known contamination changes materially?
23. Should the planning, grid and energy advantages given to AI Growth Zones be conditional on enforceable UK rights to reserve capacity in an emergency, to know who uses it and for what, and to restrict foreign military or intelligence use?
24. How exposed are UK public services and businesses to decisions by foreign governments that can switch off AI services or computing capacity, wherever the data centre is located?
25. Where a data centre's maximum water demand is many times its expected normal use, what should be required to show that the maximum can be met in a drought without affecting other users, and who should verify it?
26. Should major data-centre proposals be required to quantify their waste heat, and to show how it will be used or why it cannot be, before a site and layout are fixed?
27. Could co-locating data centres with heat networks or commercial glasshouses, and reusing treated water for irrigation, contribute to food security, and should planning policy encourage it?
28. Which public bodies in Wales use data-analytics or data-platform software supplied by US-headquartered companies for identifiable public-sector data, and what audit, insider-access and exit arrangements apply?
29. What lessons should UK and Welsh governments draw from the United States' experience in 2025 and 2026, where, according to a Justice Department court filing, sensitive public records were shared outside normal security controls by people given wide administrative access?

30. Given the Government's own acknowledgement that AI is not yet well understood, what evidence justifies accelerating AI infrastructure, through AI Growth Zones and streamlined planning, while statutory safeguards for AI remain unlegislated?
31. What assessment has government made of the energy, water, land and carbon costs of the AI computing capacity it is promoting, and will that assessment and the advice of the AI Energy Council be published?

These questions do not presume particular answers. They identify topics where further research, evidence and policy development may be required.

20. Practical Assessment Framework

Fifteen Questions Every Major Data-Centre Proposal Should Answer

1. What demonstrable need does the facility serve?
2. Why is this site preferable to reasonable alternatives?
3. What are the implications for local and national energy infrastructure?
4. What are the annual and peak-period water requirements?
5. Has the chosen cooling system been fully justified?
6. Have lifecycle emissions been assessed?
7. Have all significant environmental and amenity impacts been evaluated?
8. How will the facility perform under future climate conditions?
9. Where are primary and backup copies of information likely to reside?
10. How are single points of failure mitigated?
11. What lasting benefits accrue to host communities?
12. Does the proposal demonstrate transparency, accountability and long-term stewardship?
13. What is the realistic long-term employment case for the proposal, once the effects of automation and AI-driven efficiency have been taken into account?
14. How much waste heat will the facility produce, and how will it be used, or why can it not be?
15. Can treated water discharges or harvested rainwater be reused safely, for example for irrigation?