Reference: 02209248

Information Requests
information.requests@ofcom.org.uk

6 July 2026

Freedom of Information request: Right to know request

Thank you for your request for information about masts, licensing & radiation monitoring in Hampshire, Waterlooville and Portsmouth.

We received this request on 8 June 2026 and we have considered your request under the Freedom of Information Act 2000 ("the FOI Act") and the Environmental Information Regulations 2004

Your request & our response

Under the Environmental Information Regulations 2004 and the Freedom of Information Act 2000, please provide the following recorded information held by your department, covering the period January 2010 to present:
1. Licensing & Deployment Data
All spectrum licences, permits, assignments, and site consents issued under the Wireless Telegraphy Act 2006 to:
BT, Vodafone, O2, Three, and all other network operators Specifically for installations, base stations, or masts located in:
Hampshire
Waterlooville
Include for each site:
Exact address / OS grid reference / postcode Operator name Frequency bands authorised (including 5G, 6G trials, and high-frequency mmWave) Maximum permitted power density / EIRP Date licence issued / modified / renewed Any conditions, restrictions, or exemptions applied Any correspondence or internal notes regarding requests to "accelerate rollout" without full independent safety testing

The current Mobile Network Operator (MNO) licences can be found here and here. These include the date of issue of the licence and last version date. However, please note they only relate to permitting deployments within the United Kingdom, they do not include any site specific locations, and only provide the frequencies and maximum transmit powers.

In reference to your request for the locations of the masts, we have considered this in light of the relevant statutory scheme. We have also considered advice from HM Government on the potential implications of disclosure of information relating to the specific location of mobile sites (and other information relating to mobile sites) in the context of national security. HM Government has raised significant concerns with Ofcom about the release of this type of information on national security grounds and has advised that disclosure of this type of information would adversely affect national security. Taking this into account, Ofcom considers that regulation 12(5)(a) of the EIR applies to your request for the location of mobile masts as we consider that disclosure of the information would adversely affect national security.

In applying this exception, Ofcom has balanced the public interest in withholding the information against the public interest in disclosing it and decided that in all the circumstances of the case the public interest in maintaining the exception outweighs the public interest in disclosure. In assessing this, under regulation 12(2), we have also applied a presumption in favour of disclosure. Annex A sets out the exception in full, as well as the factors we considered when deciding where the public interest lay.

Most MNOs also have additional non-mobile Wireless Telegraphy licences used for providing backhaul services and other functions which can be found here. This information provides the location of the transmitter, maximum permitted power, licence issue date.

2. Monitoring & Measurement Results All actual field measurement data, audit reports, and compliance checks taken at ground level, residential properties, schools, and public spaces in the above areas. Include:
Exact date, time, and location of reading Frequency measured Power density / field strength readings Distance from antenna Whether readings were taken at full load or idle Any reports showing levels approaching or exceeding safety limits, or evidence that current standards are outdated or insufficient

3. Safety & Policy Records All risk assessments, internal briefings, or advice relating to the environmental and public health impacts of high-frequency electromagnetic radiation Any records discussing whether current exposure limits adequately protect wildlife, insects, soil biology, plant health, or long-term human neurological/DNA effects All correspondence with Defra, UKHSA, government, or operators regarding the adequacy of testing before deployment Defra has confirmed it holds no operational licensing or site-specific measurement data; this is a core function of Ofcom. There is strong public interest in transparency regarding the location, power, and safety of these installations in residential areas.

In response to questions 2 and 3, Ofcom periodically carries out electro-magnetic field (EMF) testing to assess the levels of EMF radiation. Results from EMF audits where MNO sites have been measured can be found here.

Additionally, the following published FOI responses may be of interest to you:

The environmental and biological risks from 5G infrastructure

5G & EMF emissions

Smart Meters, EMF and Biological Environments

ICNIRP compliance distances

We consider the remainder of the information requested, that is not already publicly available, is exempt under section 12 of the FOI Act. Section 12 of the FOI Act provides that a public authority is not obliged to comply with a request for information if the authority estimates that the cost of complying with the request would exceed the “appropriate limit”. The appropriate limit is set out in the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004, and is, for Ofcom, £450, which is equivalent to 18-hours. That sum is intended to cover the estimated costs involved in determining whether Ofcom holds the information requested, identifying, locating,

retrieving and extracting the information from any document containing it. The Regulations provide that costs are to be estimated at a rate of £25 per person per hour.

In order to satisfy your request and provide the required information, we would need to collect information from a number of different Ofcom databases and archives, then extract the information only related to the specific geographic areas requested. In some cases we would also need to search historic consultation documents, statements and emails. This would take us beyond the 18-hour limit of complying with a request.

You may wish to consider submitting a narrower, more focused request, for example, a specific topic, or type of licence/technology. We would then consider this under the FOI Act. However, should you decide to make a further request for information, please note that the aforementioned appropriate limit and/or other exemptions may apply.

Yours sincerely,

Information Requests

Request an internal review

If you are unhappy with the response you have received to your request for information, or think that your request was refused without a reason valid under the law, you may ask for an internal review. If you do, it will be subject to an independent review within Ofcom. We will either uphold the original decision, or reverse or modify it.

If you would like to ask us to carry out an internal review, you should get in touch within two months of the date of this letter. There is no statutory deadline for us to complete our internal review, and the time it takes will depend on the complexity of the request. But we will try to complete the review within 20 working days (or no more than 40 working days in exceptional cases) and keep you informed of our progress. Please email the Information Requests team (information.requests@ofcom.org.uk) to request an internal review.

Taking it further

If you are unhappy with the outcome of our internal review, then you have the right to complain to the Information Commissioner's Office.

Annex A

Regulation 12(5)(a) of the Environmental Information Regulations 2004

Regulation 12(5)(a) of the Environmental Information Regulations 2004 – a public authority may refuse to disclose information to the extent that its disclosure would adversely affect international relations, defence, national security or public safety.

The regulation is engaged because disclosure of this information would adversely affect national security.

The public interest test

Regulation 12(5)(a) is subject to the public interest test.

Key points:

- Ofcom can refuse to disclose information under this exception only if in all the circumstances of the case the public interest in maintaining the exception outweighs the public interest in disclosing the information. In assessing this, under regulation 12(2), Ofcom must also apply a presumption in favour of disclosure.
- In carrying out the public interest test, Ofcom should consider the arguments in favour of disclosing the information and those in favour of maintaining the exception, attaching the relative weight to each argument (for and against disclosure) to decide where the balance of public interest lies.
- We have set out the matters Ofcom have considered in reaching its decision with respect to the public interest below.

Factors for disclosure	**Factors for withholding**
• Transparency: There is always a general public interest in transparency. The EIR implements EU Directive 2003/4/EC on public access to environmental information. Recital 1 of the preamble to the Directive states this public interest: *"Increased public access to environmental information and the dissemination of such information contribute to a greater awareness of environmental matters, a free exchange of views, more effective participation by the public in environmental decision-making and, eventually, to a better environment."* • **Accountability:** Mobile sites produce electromagnetic fields (EMF) or radio waves. At high enough levels, EMF can impact public health. As a result, the UK Health Security Agency (previously known as Public Health England (PHE)), an expert health body, advises that spectrum users should ensure that EMF levels comply with the internationally	HM Government has advised Ofcom that: • Disclosure of this type of information raises significant concerns on national security grounds and would adversely affect national security. • Specifically, disclosure of this type of information would create an increased threat to the UK's Critical National Infrastructure (CNI). CNI is those critical elements of infrastructure (including assets, facilities, systems, networks or processes), the loss or compromise of which could result in major detrimental impact on the confidentiality, integrity, and availability of networks, or delivery of essential services (including those of the emergency services). • Government has strong concerns about publishing this type of information and has advised that publishing information on mobile sites constitutes a security risk (in particular, publishing aggregated information in a single dataset).

agreed levels in the ICNIRP Guidelines. Some individuals may have concerns about the potential health effects of EMF and want to know the location of any mobile site in their local area and whether the EMF levels from such mobile sites comply with the levels in the ICNIRP Guidelines. • **Information already in the public domain:** Some local planning authorities have published information on the location of mobile sites (including on proposed sites). Information on mobile site locations is also available on some open-source websites and mobile network operators' (MNOs) websites may indicate the general location of some masts (as well as future roll-out plans). • The location of mobile sites and other technical data is published in some other countries including in Ireland, France and Australia[1].	• Government's concerns centre on four areas: 1. **Espionage/sabotage:** Publishing this type of information could enable an attacker to remotely survey which mobile sites would be of interest from an espionage, sabotage or disruption perspective (in particular if we were to publish information relating to a large number of mobile sites in the UK). 2. **Jamming:** Publishing this type of information could enable the jamming of radio signals. 3. **Physical security:** Information relating to hub sites (mobile sites that act as their own radio coverage site and also serve to 'daisy chain' other sites), switch sites, and data centres would be of particular concern from a national security perspective. The physical security of hub sites will become even more important as features such as Mobile Edge Computing become widely available. 4. **Developments in emergency services communications**: In the future, knowledge of commercial networks could help enable an attacker to target the UK's emergency service communications network to a degree that knowledge would not have enabled in the past. This is due to the Emergency Services Network programme switching emergency service communication from the private Airwave network to a commercial network. • Government has acknowledged that where detailed technical information is not requested, an attack is more difficult. However, site location provides the starting point for an attack to gain and build additional and more detailed information that may then make any subsequent attack more likely to succeed.

[1] http://siteviewer.comreg.ie/#explore (Ireland); https://www.cartoradio.fr/index.html#/cartographie/stations (France); https://web.acma.gov.au/pls/radcom/site_proximity.main_page/ (Australia).

	Taking into account the factors in favour of disclosure, and Government's advice, we have also taken into account the following: • We consider the national security risks associated with disclosing the location of mobile sites in a single, aggregated and user friendly data set to raise a different and higher national security risk than the ad hoc disclosure of some mobile site locations as part of a planning process. We also consider that relying on information published by planning authorities is, for example, likely to make it much harder for a bad actor to coordinate an attack. This is because there may be incomplete information held by planning authorities, information may be difficult to obtain from the planning authorities and it is likely to take a significant amount of time to build up any meaningful dataset. For example, some local planning data has not been updated for several years. Further, MNOs' websites only provide general location information and do not disclose specific site locations. • Current open-source options are of much more limited use to a potential attacker than the data being requested - the data set being requested has the potential to be more damaging due to both its granularity and authoritative status. • On accountability, we do not set EMF safety levels, but we do carry out proactive testing of EMF levels near to mobile sites to check they comply with the internationally agreed levels in the ICNIRP Guidelines. Our website provides information on recent testing and measurements of EMF levels that we have taken near mobile sites. Our published measurements have consistently shown that EMF levels are well within the internationally agreed levels in the ICNIRP Guidelines. We also provide a service where individuals can request Ofcom to carry out EMF measurements near mobile sites.

	• There have been a significant number of attacks on mobile sites in recent years and publishing information on the location of sites risks further sites being attacked. Such attacks always have an adverse impact such as customers losing mobile signal and mobile operators incurring additional costs but they can have severe consequences, for example, where a mobile site that supports critical communications for the emergency services is attacked; the impact can be particularly serious in the current climate if there is disruption to a hospital's communications systems. Such attacks can also cause physical harm to employees of mobile operators, emergency services personnel and the general public.

Reasons why public interest favours withholding information

- The greater likelihood of the adverse effect, the greater the public interest in maintaining the exception. This is affected by how extensive the adverse effect is – in this case the adverse effect on national security has the potential to affect the security of the United Kingdom and its people, and the opportunity for the adverse effect to arise is ongoing.
- The impact of the adverse effect on national security also has the potential to harm the United Kingdom and its people and is therefore severe.
- The open-source information that provides similar data may present inaccurate, partial or out-of-date data, which makes them of much more limited use to a potential attacker. Using these open-source information websites would not yield the same level of accuracy as would be contained in the information requested.
- Much of the other publicly available data does not disclose specific site locations or has not been updated for several years and is similarly likely to be inaccurate and incomplete.
- The security risk is also materially higher when all of the requested information is aggregated into a single user-friendly dataset, and published.
- We have carefully considered whether the arguments around transparency and accountability may outweigh the arguments in favour of withholding the information. In doing so, we have taken into account the national security risks identified above as well as (i) the fact all of our EMF measurements to date have shown that EMF levels are well within the internationally agreed levels in the ICNIRP Guidelines; and (ii) the high risk of attacks on mobile sites which can have significant adverse consequences.
- On balance, the arguments against disclosure – including the likelihood and severity of the adverse effect on national security, and the increased threat to national security in respect of the requested information when compared to the information already in the public domain - carry greater weight than the arguments in favour of disclosure. Therefore, the public interest in maintaining the exception outweighs the public interest in disclosure.

- We also note that on 24 September 2024 the Information Commissioner's Office upheld Ofcom's decision to withhold the disclosure of mast locations on the grounds of national security in the context of an appeal of Ofcom's application of the national security exception.