Government
Property
Agency

GPA WiFi Connection Privacy Notice

This document explains how and why the GPA collects WiFi connection data from mobile devices at our sites.

The Government Property Agency (GPA) is an executive agency of The Cabinet Office, and our key role is to provide ‘great places to work’ for Government Departments.

The GPA Workplace Strategy 2020-2030 sets out our goals for improving the workplace experience for civil servants and our commitment to optimise transformational change within the Government Estate.

Part of our approach is to use technology to better understand how the workforce operates within our sites, and how effectively the facilities and spaces within our buildings are being used.

WiFi connection data provides valuable insight in this respect, allowing us to analyse trends and patterns in terms of building use, enabling us to plan how we can meet the workplace needs of a dynamic civil service going forward.

What is WiFi connection data?

When a mobile device such as a smartphone, laptop or tablet has Wi-Fi enabled, the device will continually search for a WiFi network to connect to. This is called a probing request.

By identifying the probing request, we can recognise that a device is within proximity of our WiFi network, and the approximate location of the device by using WiFi signal strength to estimate the location of the devices our network can see.

Our network can see both devices that are connected to our WiFi network, and devices that are not currently connected but searching for networks to connect to.

When connected to our network, devices will share identifying information which is specific to the device, in particular its Media Access Control (MAC) address.

Our systems then process that data to give us aggregated information related to how many devices are onsite, directions of workforce travel around the building, areas that are under or over populated and other indicators that assist the GPA with real-time location management and forward workplace enhancement planning.

This is what we mean by connection data.

We only use data about devices that connect to our network for our analysis to improve the operation of the building. Data from probing devices that do not connect is collected by the network, but not included in our analysis.

How we collect it

When you are near or inside one of our buildings and you have WiFi enabled, your device will send a probing request to connect to our WiFi every 1 minute, and your device will be visible to the network.

This probing request will be recognised by our WiFi connection data system, even if your device does not connect to our or any other WiFi network. The probing request is enough for us to recognise that a device is present.

The network automatically collects data about both probing and associated connected devices, although we only use data about associated devices in our analysis.

This data collection is carried out independently by the GPA, who are the Data Controller..

Is any Personal Data collected?

When collecting the location details of mobile devices on our network, the MAC address of the device is processed (personal data). We store and process anonymised identifiers derived from a device's MAC address as part of our analysis of location data.

A random, temporary IP Address (personal data) is also created by the system and allocated to the device via a process known as DHCP. We take steps to minimise the length of time that a particular IP address is associated with a particular device in order to reduce privacy risks, however because of the way DHCP works we cannot guarantee that an IP address won’t be retained by a device for an extended period.

This information is logged by the network however it is not used as part of our analysis for location services. IP addresses are removed from location data processing at the earliest opportunity.

The device name (personal data) is collected by the network as a routine part of operation. Although this information is retained by the network as part of its normal operation we do not store device names as part of our analysis of location data. Device names are removed from the location data processing at the earliest opportunity.

No other personal data is collected. The WiFi connection data system does not record phone numbers or browser activity, does not record the WiFi service that a device may connect to, or record any other data which could identify a living person.

How we make sure we can't identify people

We will not be able to identify any individuals from the data collected.

We are using technology to understand how the workplace is being used by the workforce population; not to monitor individuals’ movements.

Identifying information is stored by the network as part of the logging data required to ensure the secure and effective operation of the network, but it is anonymised by the network by hashing* as part of the network's location analysis capabilities. The network stores a partial hash of the device's MAC address.

Where location data is processed by the GPA as part of wider analysis for occupancy analysis, GPA's hashing capability is designed to prevent analysis across multiple days. All other personal data is removed from the processing chain at the earliest opportunity and no other identifiers are stored.

Where we are processing WiFi connection data for occupancy analysis, the identifier is processed to derive occupancy calculations (an estimate of the number of people at a given location) and then discarded. The anonymised identifier is not stored by the system.

We are unable to identify any individuals from information presented in dashboard form to the GPA.

* Hashing is the process where data is transformed into a shorter version, or given a new identifier, to process within a table or dataset. Hashing makes the identification of an individual much harder.

Preventing processing

Signs are in view at GPA Buildings explaining that the collection of WiFi connection data is taking place, however, if you would like to stop your mobile device from being part of this collection, you can turn off WiFi on your device, turn your device off or put the device into airplane mode while onsite at a GPA building.

You may also contact the GPA Data Protection Team for more information about the processing and if you have any queries or concerns about how we process personal data. See contact details section below.

Why the GPA is doing this

WiFi connection data helps us to understand how the buildings are being used.

This data allows us to identify which parts of the estate are 'over' or 'under' used in capacity terms, at what times and how this changes on a daily, weekly, monthly or annual basis.

This knowledge and data allows us to plan and provide onsite workplace improvements for the civil service. It provides constantly updated information for the GPA to deliver better capacity planning and resource management.

Legal basis for using this information

Under UK Data Protection Legislation, the GPA is only allowed to use personal information if we have a proper reason or 'lawful basis' to do so.

In the case of WiFi connection data, our 'legal basis' for processing this data is:

- Legitimate Interest (UK GDPR, Article 6, clause 1f)

Length of time we keep WiFi connection data

GPA will retain any data collected in line with our data retention policies. This means that we will not hold information for longer than is necessary for the purposes we obtained it for.

The network stores location data for a period of 6 months.

When this retention period is over, only aggregated data will be held. Aggregation enables us to understand patterns and movements over time and ensures that individual de-personalised data does not need to be held.

Aggregated data results in the individual WiFi connection data being removed. Instead, we will retain data relating to patterns grouped into specific time periods and locations.

There are process controls in place to make sure that aggregated data is at a crowd level only. Any data relating to totals of fewer than five will not be included. This will ensure that GPA does not unintentionally identify any individual, or have the realistic capacity to do so.

Keeping information secure

We take the privacy of individuals very seriously. A range of policies, processes and technical measures are in place to control and safeguard access to, and use of, WiFi connection data.

Anyone at the GPA with access to this data has been vetted and possesses security clearance.

Sharing information

WiFi connection data is accessible only to a controlled group of GPA employees, plus third-party suppliers involved in the system delivery who either host or process the data, subject to strict data protection and security controls. *Please contact the GPA Data Protection Team for more details.*

Aggregated data may be shared with GPA management or other external bodies. No personal data will be included if shared in this way.

We understand that there may be rare scenarios where the data could be useful to the police and other law enforcement bodies. As with current processes for other data held, when we get a request to disclose data, we require the police to demonstrate that the data concerned will help them to prevent or detect crime and/or prosecute offenders. Requests will be dealt with on a strictly case-by-case basis to ensure that any disclosure is lawful.

Your information rights

The GPA manages personal data in line with the requirements of the Data Protection Act (2018), including UK General Data Protection Regulation (UK GDPR).

The rights under Articles 15 to 20 of UK GDPR do not apply if the GPA is not in a position to identify a specific individual to whom the personal data belongs, unless the individual provides additional information to enable identification.

Please note that only providing a MAC address does not establish a definite link between any individual and a device.

Even where we can associate a particular device with an individual, we cannot assume the same individual was in possession of the same device on that day. It would not be practical or proportionate to establish who was carrying the mobile device at each point in time.

This means that we are unable to provide personal data in response to any requests to access the WiFi data generated by your device.

Please also refer to the guidance above on how to choose not to provide your device's WiFi connection data.

Please contact the GPA Data Protection Team (details below) for further details about the systems that process and collect WiFi connection data, and your rights under UK GDPR.

GPA Data Protection Team

You can make an enquiry, or action your Data Rights by making a valid subject access request (SAR) to the GPA, who are the data controller of your personal data.

Contact the GPA to action a subject access request (SAR) via post or email.

GPA Data Protection team
Government Property Agency
23 Stephenson Street
Birmingham
B2 4BH

Email. dataprotection@gpa.gov.uk

- Please be specific in your request, clearly explaining what you are asking for and ensure that you have provided means for us to positively identify you.
- We are prohibited from releasing personal data to any individual, unless we are sure it is the personal data solely of the individual actioning the SAR.
- We cannot release personal data to a third party, organisation or family member without prior written consent from the data subject.
- We are prohibited to release personal data of multiple data subjects to one individual.
- We will respond within 30 days – unless we contact you to indicate a valid reason why we need to extend this period, in line with data protection legislation parameters.

Data Protection Officer

If you require further information regarding the GPA's data processing activities, the contact details for our Data Protection Officer (DPO) are:

Data Protection Officer
Cabinet Office
70 Whitehall
London
SW1A 2AS
dpo@cabinetoffice.gov.uk

The Data Protection Officer provides independent advice and is charged with monitoring the GPA's use of personal information.

Information Commissioner’s Office (ICO)

If you consider that your personal data has been misused or mishandled, you may make a complaint to the Information Commissioner, who is the UK’s independent regulator and Supervisory Authority.

The information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Telephone: 0303 123 1113
casework@ico.org.uk

Any complaint to the Information Commissioner is without prejudice to your right to seek redress through the courts.