

CAPITA

Capita IT and Networks General Privacy Notice

January 2019

V1.2

Table of Contents

| | |
|--|----|
| Table of Contents..... | 2 |
| 1. Who are we? | 3 |
| 2. Whose data do we process? | 5 |
| 3. Where we might capture Personal Data? | 6 |
| 4. Why do we process Personal Data?..... | 8 |
| 5. What data do we process? | 9 |
| 6. Where do we process the data? | 11 |
| 7. How long do we keep the data for? | 12 |
| 8. Who will we share data with? | 13 |
| 9. Personal Data processed by 3 rd parties..... | 14 |
| 10. Security | 15 |
| 11. Changes to Business Organisation | 16 |
| 12. Access to personal information | 17 |
| 13. Complaints or queries | 18 |
| 14. Your rights..... | 19 |
| 15. Disclosure of personal information | 20 |
| 16. Changes to this Privacy Notice..... | 21 |

1. Who are we?

We are Capita IT and Networks and we provide IT services to business clients. These services include;

- Application Management
- Cloud and Infrastructure Management
- Customer Engagement
- Intelligent Buildings
- Networks
- Structured Cabling
- Fibre optic Cabling
- Data Centres
- Testing Services (including Vulnerability & Penetration Testing)
- IP Security
- Defence and Security
- Cyber Security
- External IT cabling infrastructure
- Service Management
- Unified Cloud and Collaboration
- Consulting / Professional Services
- Break Fix Services

We also trade as;

- **Capita Business Services Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Capita IT Services Limited**
(registered address is Pavillion Building, Ellismuir Way, Tannochside Park, Uddington, Glasgow, G71 5PW)
- **Capita IT Services (BSF) Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Capita Intelligent Buildings Infrastructure Services Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Capita Managed IT Services Limited**
(registered address is Hillview House, 61 Church Road, Newtonabbey, Co. Antrim, BT36 7LQ)
- **Trustmarque Solutions Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Pervasive Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Electra-Net UK Ltd**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Electra-Net Group Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Network Technology Solutions (UK) Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Westpoint Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Acutest Limited**
(registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)

- **Updata Infrastructure (UK) Limited** (registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)
- **Daisy Updata Communications Limited** (registered address is Daisy House Suite 1, Lindred Road Business Park, Nelson, Lancashire, BB9 5SR)
- **Pervasive Networks Limited** (registered address is 30 Berners Street, Fitzrovia, London, W1T 3LR)

We can be contacted in connection with this notice at CapitalTandNetworksPrivacy@capita.co.uk.

Our website is <https://www.capita-it.co.uk/>.

This privacy notice was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be sent to the address or email above.

2. Whose data do we process?

As a Data Controller

We process Personal Data of the following groups of people;

- Employees, ex-employees and potential employees
- Visitors to our places of work
- Individuals in our customers' organisations
- Individuals in our suppliers' organisations
- Visitors to and users of our websites
- Specialists with whom we engage to deliver particular projects
- Users of the systems that we provide
- Callers to our telephone systems
- People who give us business cards
- People included on purchased marketing lists
- Customers
 - When we are the Data Controller, we process information obtained directly from our customers such as name, address, billing information, and some employee contact information. We may also collect other information about the customer and some employees, for example through our web sites and service interactions, as part of that data. We know that information as Customer Data.

As a Data Processor

- Capita IT and Networks provides services to clients which include the processing of Personal Data relating to the client, the client's staff or the client's customers. In these cases, the client is the Data Controller and we are the Data Processor. As Data Processor, we process the Personal Data on behalf of the Data Controller and under their instructions, as agreed in our contract.
- We may also process Personal Data as a Sub-Processor. This means that we have been engaged by the Data Processor to process Personal Data under their instructions as part of the role of delivering services to the Data Processor, as agreed in our contract.
- When we are a Processor, we process information in accordance with the instructions that we have in the contract or service order. When we provide a service, the data is classified and handled in accordance with the terms of the contract or the order for those services. The data processed by the service provided, or processed to provide the service, is known as Services Data.
- When we are a Data Processor the privacy policy for the services data will be included in the service and contract documentation.

3. Where we might capture Personal Data?

- From our websites
 - Individuals can contact us using functions provided on our and we capture personal information (for example email addresses, IP addresses, names, address, job title) in connection with that communication.
 - Individual websites will have their own privacy policy, detailing exactly what is processed by that particular website.
- From our sales order processing systems
 - Business contact information, billing details, order details.
- From our customers
 - Customers provide us with lists of authorised business contacts for the functions we are contracted to provide.
 - Feedback on the performance of our staff in connection with contracted services.
 - Voice recording of service calls for performance and training purposes.
- From third party marketing companies (i.e. purchased marketing lists or provided to us by our business partners)
 - Business contact details.
- From suppliers, partners and contractors where it is necessary to provide their contracted services
 - Names, contact details and previous experience of employees and specialists involved in delivering the services.
- From events, conferences and exhibitions we attend, either from personal contact or from the organisers and promoters (e.g. business cards and attendee lists)
 - Business contact details.
- From details provided to us by individuals
 - Business cards
 - Telephone calls
 - Correspondence
 - CV's.
- CCTV.
- Voice recording of telephone calls.
- From potential employees, including contractors, during the recruiting process.
- CVs when people are referred to us by colleagues or other contacts.
- When people log in as "Guest" to our WIFI networks.
- When people park in our carparks.
- When people sign in to our visitor's books.

-
- For secure sites, when people provide further details to enable us to identify them.
 - From our staff, for employment reasons.
 - From our staff, for security purposes.
 - Investigations following an incident e.g. security and or health and safety.
 - Lists of people who are or have attended networking events, usually from organiser / promoter.

4. Why do we process Personal Data?

We process Personal Data where it is necessary for the following purposes;

- To assist in the running of the company; including, but not limited to invoicing, billing, arranging visits and internal record keeping.
- For employment and recruitment purposes, including identifying suitable specialist's contractors for certain project.
- To fulfil our contracted relationships, provide goods and services to our customers and answer queries.
- For security and prevention of crime (CCTV).
- For Safety, Health and Environment incident monitoring and prevention.
- To market ourselves to other businesses using named individuals within those businesses, and to reply to individuals who have contacted us.
- To improve our products and services;
 - Using feedback provided by individuals
 - For training and quality purposes (voice recording)
 - Legal and regulatory reasons e.g. HMRC and regulatory reporting.

5. What data do we process?

Running our Company

We process the necessary information in our legitimate interests;

- To fulfil our contracted relationships, provide goods and services to our customers, answer queries, obtain payment (invoicing, billing process), arrange visits, or during internal record keeping
 - Business contact details
- To improve our products / services
 - Using feedback provided by individuals
 - For training and quality purposes (voice recording)
- To carry out vetting and/or credit checking of potential employees, customers and suppliers (such as contractors)
- To satisfy our clients security requirements we provide a vetting service for HMG BPSS which includes the following fields: -
 - Name, address and contact details
 - Residence and employment history
 - Nationality
 - Criminal history

Employee and recruitment data

For information regarding the processing of employee data, please contact privacy@capita.com.

Current employees should refer to the Employee Handbook.

CCTV

We may use CCTV to record images at any of our locations at any time. We may also use monitored CCTV systems in some of our locations. These images may be of any person present at our locations.

The purpose of this CCTV is for the safety of the public and staff at these locations, and to prevent and detect crime. In locations that have CCTV there are signs displayed notifying you that CCTV is in operation.

Marketing Information

- We use marketing information in our legitimate interests to reach other businesses and do not market to private individuals.
- We use information known to us as business contact details (name, role, telephone number, email and physical address) to provide details of goods and services that we believe may be of interest to you.

To fulfil our legal requirements

- Safety, Health and Environment incident monitoring and prevention
 - We keep details of Safety, Health and Environment incidents, near misses and assessments to keep our staff and members of the public safe, and in accordance with SHE legislation.
 - We may use CCTV images for the purposes of SHE incident monitoring and prevention.
- Where we believe it is necessary to comply with any law enforcement agency, court, regulator or official registrar (such as the Financial Conduct Authority or Companies House), or government authority, we may process your Personal Data to meet our obligation. Examples of this are to fulfil our obligation with regards to tax regulations, or to equal opportunity monitoring.

Special categories of data

- We may process certain special categories of Personal Data (which are defined as Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation).
- We may also process Personal Data relating to criminal convictions and offences, which are not special categories of Personal Data but are subject to special rules under the GDPR.
- In line with our obligations as an employer, we will use your particularly sensitive personal information in relation to;
 - leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
 - your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
 - your race or national or ethnic origin, religious, philosophical or moral beliefs, or your gender, to ensure meaningful equal opportunity monitoring and reporting.
 - any criminal convictions, police cautions, court appearances (including in respect of country court judgements), civil disputes, bankruptcy proceedings and individual voluntary arrangements etc. in deciding if a candidate or employee is appropriate for a role.

6. Where do we process the data?

- We process Personal Data in our offices and data centres in the UK.
- We also process some Personal Data in our offices in the Republic of Ireland, Poland and in India.
- In accordance with good practice, and because it is outside the EEA, all engagements with India are underpinned by suitable Inter-company agreements.

7. How long do we keep the data for?

We keep Personal Data for no longer than it is needed, and in accordance with our Data Retention Policy.

Examples of this might be:

- for as long as your account is active
- as needed to provide you with products or services
- as needed for the purposes outlined in this Policy or at the time of collection
- as necessary to comply with our legal obligations (e.g. to honour opt-outs)
- resolve disputes, and enforce our agreements
- or to the extent permitted or required by law.

At the end of the retention period, we will delete your Personal Data in a manner designed to ensure that it cannot be reconstructed or read.

8. Who will we share data with?

In the running of our business, we sometimes work closely with other organisations. Your personal information may be passed to one of these organisations when required to perform the service. However, Capita IT and Networks will still be responsible for your information, its security and what happens to it.

In addition to this, we may be required by law to share your information with some of these organisations.

Typically, depending on the circumstances, we share information with the following types of organisations;

- Contracted third parties where the information shared is necessary to provide the service
- Law enforcement agencies such as the Police, and Fire and Rescue Service
- Other government / regulatory agencies as required by law
- Our external auditors
- Customers, where we are providing people to work with and for them (e.g. identification information, CV info, qualifications, certifications and security vetting)
- Other Capita Group companies. We share Personal Data when it is necessary among our group companies. All group companies are required to comply with equivalent privacy notice obligations.
- Our Vetting and credit checking partners.

Where we do share your information, we will take steps to ensure that those it is shared with keep your information secure, and that they also comply with legislation. The work will be underpinned by appropriate commercial agreements.

9. Personal Data processed by 3rd parties

Where we have contracted Personal Data processing to a third party, we have contracts in place with our Data Processors. This means that they cannot do anything with your personal information unless we have instructed them to do it. They will not share your personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct.

Credit Checks and Security Vetting

We may enter in to arrangements with other companies to provide credit checks and security vetting, where although we are commissioning a service, they will also act as Data Controller for the data that you provide and will determine the purpose and manner of processing. Where this happens, you will be informed when you provide the data.

10. Security

We are committed to the security of all Personal Data and have various policies and tools in place to ensure the physical, administrative and technical security of all data in our care, which includes Personal Data. We use security practices and operating procedures that are compliant with standard industry practices or other practices as defined in the relevant service description or contract document (as applicable).

Where relevant and applicable we obtain external certifications such as ISO 27001, ISO 22301, PCI DSS, and CyberEssentials.

We also require that our third-party partners and suppliers protect any Personal Data that they process from unauthorised use, alteration, loss and disclosure.

11. Changes to Business Organisation

We may from time to time, expand or reduce our business and this may involve a reorganisation of our business operations, including buying new businesses or selling or merging existing businesses. This may involve us disclosing Personal Data to prospective or actual purchasers of parts of our business or receiving Personal Data from potential sellers. We will obtain appropriate confidentiality protection for Personal Data disclosed in these types of transactions.

Relevant Personal Data will be transferred along with that division and the new owner or newly controlling party will be permitted to use the data for the purposes for which it was obtained.

12. Access to personal information

Individuals can find out if we hold any personal information about them by contacting CapitalTandNetworksPrivacy@capita.co.uk.

If we do hold information about you, we will;

- Give you a description of it
- Tell you why we are holding it
- Tell you who it could be disclosed to
- Let you have a copy of the information in an intelligible form.

To make a request for any personal information we may hold you need to put the request in writing using the email address CapitalTandNetworksPrivacy@capita.co.uk or writing to the address provided in the “who are we” section of this Notice.

If you agree, we will try to deal with your request informally, for example by providing you with the specific information you need over the telephone.

If we do hold information about you, you can ask us to correct any mistakes by using the contact details in the “who are we” section of this Notice.

13. Complaints or queries

We aim to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you want to make a complaint about the way we have processed your personal information, you can request a formal internal investigation by contacting privacy@capita.com. You can also contact the body that oversees Data Protection in the UK – the Information Commissioners Office at <https://ico.org.uk/>.

14. Your rights

You have the right to be informed about how we will use your information. You also have the right (free of charge) to the following;

- Access to any personal information we hold about you.
- To have your information corrected if there are inaccuracies or if the information is incomplete.
- To restrict the processing of your information in certain circumstances in accordance with applicable law.
- In some instances, to object to your personal information being used at all due to special grounds relating to your situation. However, there may be compelling reasons why we may need to continue using your information even in these circumstances.
- To be told if your personal information is lost and if as a result, your privacy and rights may be at risk.

In addition to the above, if we have no legal basis to process your information other than the fact that you gave us your consent, then you have the following additional rights;

- To withdraw your consent to process your information.
- In some instances, to ask for your personal information to be sent to another organisation in a suitable format. For example, we can provide you with your personal information in a structured, commonly used, machine readable form when asked.
- To withhold permission for your information to be shared.

15. Disclosure of personal information

There are circumstances in which we may need to share Personal Data. We will not disclose Personal Data without a legal ground to do so and in connections with reason or which we process the data.

You can also ask us further information on;

- Agreements we have with other organisations for sharing information.
- Circumstances where we can pass on Personal Data without consent for example, to prevent and detect crime and to produce anonymised statistics.
- Our instructions to staff on how to collect, use and delete Personal Data.
- How we check that the information we hold is accurate and up to date.

16. Changes to this Privacy Notice

We keep our Privacy Notice under regular review.

This Privacy Notice was last updated in January 2019. It will be reviewed annually, with the next review due in January 2020.

It may be changed during the year, for example if we introduce a new service, to make sure that it is always current and complete.