CLOUDSCAPE IT LTD

Privacy Policy

How we collect, use and protect personal information

Last updated	24/8/2026
Version	1.5
Applies to	cloudscapeit.co.uk and all Cloudscape IT Ltd services
Governing law	England and Wales

1. About this policy

Cloudscape IT Ltd ("Cloudscape", "we", "us", "our") is committed to protecting the privacy of everyone whose personal information we handle. This policy explains what personal information we collect, why we collect it, what we do with it, how long we keep it and what rights you have.

It applies to visitors to our website, prospective clients, clients and their staff, our suppliers, job applicants and anyone else who contacts us. It also explains the separate role we play when we handle personal information on behalf of our clients as part of our managed IT services - see section 3.

We are the data controller for the personal information described in this policy, unless we say otherwise. Our details are:

Company	Cloudscape IT Ltd
Registered number	04565979 (England & Wales)
Registered office	47 Oxford Drive, Magdalen Street, London SE1 2FB
Email	privacy@cloudscape.it
Telephone	0207 952 8123
ICO registration	ZA346334
Data protection contact	Mike Casey

We follow UK data protection law, principally the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, both as amended by the Data (Use and Access) Act 2025, together with the Privacy and Electronic Communications Regulations 2003 (PECR).

2. A quick summary

The detail follows, but in short:

- We collect personal information when you use our website, contact us, become a client, apply for a job or supply services to us.
- We use it to respond to enquiries, deliver and support our services, run our business, keep our systems secure and - where permitted - tell you about services that may interest you.
- We do not sell your personal information, we do not share it with third parties for their own marketing.
- We keep it only as long as we need it, then delete or anonymise it.
- You have rights over your information, including the right to see it, correct it and object to how we use it.
- You can complain to us directly, we will acknowledge your complaint within 30 days. You can also complain to the UK data protection regulator.

3. Our two roles: controller and processor

This distinction matters, it is the part most people miss when reading an IT provider's privacy policy.

When we are the controller

For the information described in this policy - website visitors, enquiries, client contacts, suppliers, job applicants and our own staff - Cloudscape decides why and how the information is used. We are the data controller, this policy governs what we do.

When we are the processor

When we deliver managed IT services, our engineers necessarily have access to systems containing personal information belonging to our clients - their staff records, their customer data, their email, their files. We do not decide why that information exists or what it is used for. Our client remains the controller; Cloudscape acts as a processor on their instructions.

In that role we handle personal information only as instructed by the client and as set out in the data processing agreement forming part of our contract with them. Our obligations there include confidentiality, appropriate security, restrictions on the sub-processors we use, assistance with data subject requests, prompt notification of any personal data breach.

If you are an individual whose information is held in a system Cloudscape supports on behalf of one of our clients, your rights are exercised against that client, not against us. If you contact us, we will refer you to them and assist them in responding.

> **SUB-PROCESSORS**
>
> Where we engage another organisation to help deliver services to a client - for example a software vendor, a cloud platform or a specialist supplier - we do so under written terms requiring equivalent protection, only where our contract with the client permits it.
>
> This applies to every supplier in the chain, including those handling equipment or media that may contain data. We maintain a record of the sub-processors we use and make it available to clients on request.

4. What information we collect

We collect different information depending on your relationship with us.

Who you are	What we typically collect
Website visitors	IP address, device and browser type, pages viewed, referring site, approximate location derived from IP, information collected through cookies and similar technologies (see section 7).
Enquirers and prospective clients	Name, job title, employer, email address, telephone number, the content of your enquiry, records of our correspondence and meetings with you.
Clients and their staff	Contact details, job role, authorisation level, service desk tickets and correspondence, system access records, billing and payment information, records of the services we provide.
Suppliers and partners	Contact details, role, contract and payment information, correspondence.
Job applicants	Name, contact details, CV, employment and education history, right-to-work information, references, interview notes and assessment results.
Newsletter and event contacts	Name, email address, employer, your subscription and engagement preferences.

Special category data

We do not routinely collect special category data (information about health, ethnicity, religion, sexual orientation, trade union membership, biometrics or genetics). Where we do - for example accessibility or dietary requirements for an event, or health information relevant to a reasonable adjustment during recruitment - we collect only what is necessary and rely on an appropriate additional condition under Article 9 of the UK GDPR.

Children

Our website and services are aimed at businesses, we do not knowingly collect personal information relating to children. If you believe we hold information about a child, please contact us and we will delete it.

5. How we collect it

- Directly from you - when you complete a form, email or call us, meet us, subscribe to our mailing list, attend an event, apply for a role or enter into a contract with us.
- Automatically - through cookies and similar technologies when you use our website, through the monitoring and management tools we operate for clients.
- From your employer - where you are a contact at a client, supplier or prospective client.
- From third parties - including recruitment agencies, referral partners, publicly available sources such as company websites, Companies House and professional networking sites, business data providers.

Where we obtain your details from a third party or a public source for the purpose of contacting you about our services, we will tell you where we got them if you ask.

6. Why we use it, our lawful basis

UK data protection law requires us to have a lawful basis for each use of personal information. Ours are set out below.

What we do	Why	Lawful basis
Respond to enquiries	To answer your question and, where relevant, prepare a proposal.	Legitimate interests (responding to those who contact us); steps prior to entering a contract.

What we do	Why	Lawful basis
Deliver and support our services	To provide managed IT services, run the service desk, manage your systems and bill correctly.	Performance of a contract; legitimate interests where the contract is with your employer.
Keep systems secure	To monitor for, investigate and respond to security threats affecting our systems and those we manage.	Recognised legitimate interest (ensuring the security of network and information systems); legal obligation.
Business administration	Accounting, invoicing, credit control, insurance, professional advice and internal reporting.	Legitimate interests; legal obligation.
Marketing our services	To send relevant updates, guidance and event invitations to business contacts.	Recognised legitimate interest (direct marketing) and, where required by PECR, consent.
Improve our website	To understand how the site is used and make it more useful.	Legitimate interests; consent where required for cookies.
Recruitment	To assess applications and manage the hiring process.	Steps prior to entering a contract; legitimate interests; legal obligation for right-to-work checks.
Meet legal and regulatory obligations	Tax, company law, responding to lawful requests and establishing or defending legal claims.	Legal obligation; legitimate interests.

A note on legitimate interests

Where we rely on legitimate interests, we have considered whether our interests are outweighed by your rights and freedoms, we have concluded they are not. You can ask us for details of that assessment, you have the right to object - see section 12.

The Data (Use and Access) Act 2025 introduced a category of "recognised legitimate interests" which do not require that balancing exercise. Where we rely on one - principally to secure our networks and information systems, for direct marketing to business contacts - we have identified it above.

7. Cookies and similar technologies

Our website uses cookies and similar technologies. Some are strictly necessary for the site to work. Others help us understand how the site is used or remember your preferences.

UK law now exempts certain low-privacy-risk cookies - including some analytics and functionality cookies - from the requirement to obtain consent, provided you are told about them and can object. For anything outside those exemptions, we ask for your consent before setting the cookie, you can withdraw it at any time.

You can manage your preferences through the cookie banner on our website, or through your browser settings. Blocking strictly necessary cookies may stop parts of the site working.

8. Marketing

If you are an existing client, or you have asked us to, we may send you information about our services, guidance we have published, invitations to events. We send these by email, occasionally by post or telephone.

We only send business-to-business marketing to people whose role makes it relevant, we make it easy to stop. Every marketing email contains an unsubscribe link, you can also email us at any time to opt out. Opting out of marketing does not affect messages we need to send you about services we are already providing.

We do not sell or rent your details to other organisations for their marketing.

9. Who we share it with

We share personal information only where there is a proper reason. The categories are:

- Service providers who support our business - including our cloud and hosting providers, professional services automation and remote monitoring platforms, documentation systems, customer relationship management system, email and productivity platform, accounting software and marketing tools.
- Professional advisers - accountants, auditors, insurers, lawyers and consultants, where they need the information to advise us.
- Vendors and partners - where a service you receive is delivered in conjunction with a third-party product, only so far as necessary.
- Regulators, law enforcement and other authorities - where we are legally required to do so, or where it is necessary to establish, exercise or defend legal claims.
- A purchaser - if we sell or reorganise part of our business, in which case your information may transfer with it, subject to the same protections.

Every supplier who handles personal information on our behalf does so under a written contract requiring them to keep it secure, use it only on our instructions, return or delete it when the arrangement ends. We assess suppliers before appointing them and review those arrangements.

A current list of the main service providers we use is available on request.

10. Sending information outside the UK

Most of the information we hold stays in the UK or the European Economic Area. Some of our service providers operate internationally, which means personal information may be transferred to, or accessed from, other countries.

Where that happens, we make sure an appropriate safeguard is in place - typically a UK adequacy determination for the destination country, the UK International Data Transfer Agreement, or the UK Addendum to the European Commission's standard contractual clauses. Where required, we carry out a transfer risk assessment applying the statutory data protection test, which asks whether the standard of protection in the destination country would be materially lower than under UK law.

You can ask us for details of the safeguards applying to a particular transfer.

11. How long we keep it

We keep personal information only as long as we need it for the purpose we collected it, or as long as the law requires. Our normal periods are below. Where a longer period is needed - for example because of an ongoing dispute - we keep the information until that concludes.

Information	Normal retention period
Enquiries that do not become clients	24 months from last contact
Client records and correspondence	6 years after the end of the contract, to match the limitation period
Financial and accounting records	6 years after the end of the financial year to which they relate (statutory)
Service desk tickets and system logs	For the duration of a business relationship and for 24 months upon cessation of a business relationship, longer where needed for an investigation
Marketing contacts	until you unsubscribe, plus a suppression record kept indefinitely so we do not contact you again
Unsuccessful job applicants	12 months, with consent for longer
Website analytics	12 months
CCTV, if operated	30 Days

When information is no longer needed, we securely delete it or anonymise it so it can no longer identify anyone. Where we dispose of equipment or media that has held personal information, we do so through a controlled process with a record of what was destroyed.

12. How we protect it

We take the security of personal information seriously, as an IT and cyber security provider we hold ourselves to the standards we recommend to clients.

Our measures include:

- Multi-factor authentication on accounts with access to personal information
- Role-based access control, with access limited to those who need it and reviewed regularly
- Encryption of data in transit and at rest on managed devices
- Managed, monitored and patched endpoints
- Network monitoring, logging and alerting
- Backups that are tested and held separately from live systems
- Staff training on data protection and information security, refreshed regularly
- Written policies covering acceptable use, incident response and the use of artificial intelligence
- Due diligence on suppliers who handle personal information, with written contractual protections
- Cyber Essentials and Cyber Essentials Plus certified

No system can be guaranteed completely secure. If a personal data breach occurs that is likely to result in a risk to people's rights and freedoms, we will report it to the regulator within 72 hours of becoming aware of it, we will tell affected individuals directly where the risk to them is high. Where we act as a processor for a client, we notify that client without undue delay so they can meet their own obligations.

13. Automated decision-making and artificial intelligence

We do not make decisions about you that produce legal or similarly significant effects based solely on automated processing.

We use AI-assisted tools in parts of our business, for example to help draft documents, summarise information and support our service desk. Where we do:

- We govern their use through a written AI acceptable use policy
- We control which tools may be used and what information may be entered into them
- We do not permit client personal information to be entered into unapproved consumer AI services
- Where AI is used in a way that affects you, a person remains responsible for the outcome and you can ask for it to be reviewed

UK law changed in February 2026 to permit a wider range of automated decision-making, provided safeguards including transparency, human review and the right to contest are in place. If our practice changes, we will update this policy and tell you.

14. Your rights

You have the following rights over your personal information. They are free to exercise, we will normally respond within one month.

- **Access -** to receive a copy of the personal information we hold about you.
- **Rectification -** to have inaccurate information corrected and incomplete information completed.
- **Erasure -** to have your information deleted, where there is no good reason for us to keep it.
- **Restriction -** to ask us to limit how we use your information while a concern is resolved.
- **Objection -** to object to processing based on legitimate interests. You have an absolute right to object to direct marketing, we will stop.
- **Portability -** to receive certain information in a portable format, or have it transferred to another organisation.
- **Withdraw consent -** where we rely on consent, to withdraw it at any time, without affecting anything done beforehand.
- **Automated decisions -** to ask for human review of, to contest, a solely automated decision with significant effects.

How to make a request

Contact us at privacy@cloudscape.it. We may ask you to confirm your identity before we respond, which protects you as much as us. Where we need that confirmation, or need to clarify what you are asking for, the one-month period starts once you have provided it.

When responding to an access request, we are required to carry out a reasonable and proportionate search rather than an exhaustive one. If your request is complex, or you have made several, we may extend the period by a further two months and will tell you why within the first month.

Some rights do not apply in every situation. If we cannot meet a request, we will explain why.

15. How to complain

If you are unhappy with how we have handled your personal information, please tell us. We would rather hear from you and put it right.

Complaining to us

You can make a data protection complaint by email to privacy@cloudscape.it, by post to our registered office.

We will acknowledge your complaint within 30 days of receiving it, we will respond substantively without undue delay. If we need more information from you to investigate, we will ask promptly. We keep a record of complaints and what we did about them, so we can learn from them.

Complaining to the regulator

You also have the right to complain to the UK data protection regulator. In most cases you will be expected to raise your complaint with us first.

Regulator	Information Commissioner's Office (transitioning to the Information Commission)
Website	ico.org.uk
Helpline	0303 123 1113
Post	Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

The regulator is being reconstituted as the Information Commission under the Data (Use and Access) Act 2025. Its powers and the protections available to you are unchanged; only the name and governance structure are changing.

16. Other websites

Our website contains links to other sites. This policy applies only to Cloudscape, we are not responsible for how other organisations handle your information. We would encourage you to read their privacy policies.

17. Changes to this policy

We review this policy regularly and will update it when our practices change or the law does. The date at the top shows when it was last updated. Where a change materially affects how we use your information, we will tell you directly.

18. Contact us

For anything relating to this policy or your personal information:

Email	privacy@cloudscape.it
Telephone	0207 952 8123
Post	Data Protection, Cloudscape IT Ltd, 47 Oxford Drive, Magdalen Street, London SE1 2FB