

Data Protection Policy

Carlisle Computer Systems

Document	Data Protection Policy
Registered entity	CARLISLE COMPUTER SYSTEMS LIMITED
Company number	14850447 (registered in England and Wales)
Registered office	6 Brunswick Street, Carlisle, United Kingdom, CA1 1PN
Website	https://carlislecomputersystems.co.uk
Data Protection Lead	Ian Irving
Contact	DPO@carlislecomputersystems.co.uk
Effective from	19 May 2026
Version	1.0

1. Who we are

Carlisle Computer Systems ("CCS", "we", "us") is a company registered in England and Wales. We provide IT support, system administration, and computer services to businesses and individuals in Carlisle and the surrounding area.

We are the **data controller** for personal data collected through our website and during the course of providing IT services to our clients. In some circumstances we may also act as a **data processor** on behalf of our business clients (for example, when administering their internal systems on their instruction). The applicable role for each engagement is set out in the relevant service agreement.

2. What personal data we collect

We collect the following categories of personal data:

From visitors to our website

- IP address, browser type, device type, referrer URL, pages viewed, time of visit. Collected through standard server logs and analytics cookies (where you consent to them).
- Information you submit through contact forms: name, email address, phone number, the content of your message.

From clients and prospective clients

- Identifying information: name, business name, role, email address, telephone number, postal address.
- Engagement and project information: scope of work, ticket history, support correspondence, invoices, payment status.
- Technical information arising from the IT services we provide: system inventory, device identifiers, account names, access credentials (handled per separate access-control procedures), system configuration data.

From our suppliers and third parties

- Contact and contracting information for our business suppliers.

We do not knowingly collect any "special category" personal data (Article 9 UK GDPR -- race, religion, health, biometric, etc.). If special category data is incidentally present in materials supplied to us by a client during the course of services, it is handled under the corresponding service agreement and only for the purpose of providing the contracted services.

3. How we use your data (purposes and lawful basis)

Purpose	Lawful basis (UK GDPR Art. 6)
Responding to enquiries submitted via the website	Legitimate interests (Art. 6(1)(f)) -- replying to your enquiry
Providing IT support and services to clients under contract	Performance of a contract (Art. 6(1)(b))
Sending occasional service-related updates to clients (system notifications, security advisories)	Performance of a contract (Art. 6(1)(b)) and legitimate interests
Sending marketing communications (e.g. via Mailchimp)	Consent (Art. 6(1)(a)) -- you can withdraw consent at any time
Invoicing, accounting, statutory record-keeping	Legal obligation (Art. 6(1)(c)) and legitimate interests
Investigating security incidents	Legitimate interests and, where applicable, legal obligation
Defending or pursuing legal claims	Legitimate interests (Art. 6(1)(f))

4. Cookies and analytics

The website uses a small number of cookies. The cookie banner on first visit explains your choices in plain language. You can change your choices at any time via the "Cookie preferences" link in the footer.

Cookie	Purpose	Type	Set by
Strictly necessary	Site navigation, security, load balancing	First-party	CCS
Analytics (if accepted)	Aggregate visitor counts and page popularity	First-party / Google Analytics	Google
Marketing (if accepted)	Mailchimp email-campaign click-tracking	Mailchimp	Mailchimp

If you decline analytics and marketing cookies, only the strictly-necessary cookies are set.

5. Who we share your data with (processors and downstream services)

We use the following third-party service providers ("processors") to operate our business. Each is contractually obliged to handle personal data securely and only on our instructions.

Processor	Role	Data shared	Location	Their privacy notice
Microsoft (Microsoft 365 / Exchange / SharePoint / OneDrive / Graph API)	Email, calendar, document hosting, business productivity	All inbound + outbound business correspondence, calendars, documents you send us	EU + UK datacentres for tenant data; some support functions globally	https://privacy.microsoft.com
Google (Workspace, Gmail, Drive, Calendar)	Where a client engagement uses Google services; access on the client's instruction	Limited to what the client engagement involves	Per Google's regional configuration	https://policies.google.com/privacy
Mailchimp (Intuit)	Email-marketing campaigns to subscribers who consent	Name, email, engagement metrics (opens, clicks)	US (Standard Contractual Clauses + UK IDTA in place)	https://mailchimp.com/legal/privacy/
Anthropic (Claude AI)	Drafting, classification, summarisation of correspondence and support tickets (under human-in-the-loop -- see AI Policy)	The text content of items submitted to the AI for processing	US (Standard Contractual Clauses + UK IDTA in place); zero-retention API path is used for client-data calls	https://www.anthropic.com/legal/privacy
ElevenLabs	Voice synthesis (if relevant to a service engagement)	The text submitted for synthesis	US (Standard Contractual Clauses)	https://elevenlabs.io/privacy-policy
GitHub (Microsoft)	Source-control and issue tracking for our internal systems and any client engagement that uses it	Code, ticket text, contributor identities	US / globally	https://docs.github.com/en/site-policy/privacy-policies
StackCP (20i / Easyhost)	Web-site hosting	Server logs, contact form submissions	UK datacentres	https://www.20i.com/legal/privacy-policy

Processor	Role	Data shared	Location	Their privacy notice
Tailscale	Private network connectivity to our admin systems (internal only; no client data flow)	Device identifiers, IP addresses, connection metadata	US (Standard Contractual Clauses)	https://tailscale.com/privacy-policy/
PayPal / Stripe	Payment processing for invoices paid online	Name, billing address, payment instrument metadata	EU + US (Standard Contractual Clauses + UK IDTA in place)	https://www.paypal.com/uk/legalhub/privacy-full , https://stripe.com/privacy
HMRC (UK tax authority)	Statutory tax reporting	Limited identifying and financial data as required by tax law	UK	https://www.gov.uk/government/organisations/hm-revenue-customs/about/personal-information-charter
Our accountants (named on request)	Bookkeeping, year-end accounts, statutory filings	Invoice + payment data, supporting records	UK	Their own privacy notice on request

International transfers

Where personal data leaves the UK to a country not subject to a UK adequacy decision, we rely on the UK International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses, plus a transfer risk assessment. Copies are available on request.

6. How long we keep your data

Category	Retention
Website enquiry forms	24 months from last contact, then deleted
Active client records	Duration of engagement + 6 years (legal limitation period)
Invoicing + accounting records	6 years from end of the relevant tax year (HMRC requirement)
Email correspondence	6 years (aligned with client records)
Marketing-list subscribers	Until consent withdrawn or 24 months of disengagement, whichever is sooner
Server access logs	90 days rolling
Backups	Encrypted at rest; rotated on a 30/90/365-day schedule

When retention expires we delete or anonymise the records under documented procedures.

7. Your rights

Under UK GDPR you have the right to:

- **Access** the personal data we hold about you ("subject access request");
- **Rectify** inaccurate or incomplete data;
- **Erase** your data, where one of the Article 17 grounds applies;
- **Restrict** processing, where one of the Article 18 grounds applies;
- **Data portability** -- receive a machine-readable copy of data you provided to us, where Article 20 applies;
- **Object** to processing based on legitimate interests or direct marketing;
- **Withdraw consent** at any time, where the lawful basis is consent. Withdrawing consent does not affect the lawfulness of processing carried out before the withdrawal.

To exercise any right, email **DPO@carlislecomputersystems.co.uk**. We will respond within one calendar month. There is no fee unless the request is manifestly unfounded or excessive.

You also have the right to complain to the **Information Commissioner's Office** at <https://ico.org.uk> or 0303 123 1113.

8. Security

We hold personal data on Microsoft 365 (UK tenant), on hardware we physically control, and on the hosting infrastructure listed in Section 5. Standard measures include:

- Multi-factor authentication on every administrator and client-facing system;
- Full-disk encryption on devices that store personal data;
- Encrypted backups, both on-site and to a UK-region offsite store;
- Role-based access control: staff access is limited to what their role requires;
- Logging of administrative actions, with periodic review;
- Patching cadence aligned to CIS / NCSC guidance.

If we become aware of a personal-data breach that is likely to result in a risk to your rights, we will notify the ICO within 72 hours and, where the risk is high, notify affected individuals.

9. Automated decision-making and profiling

We do not make decisions about you that have legal or similarly significant effects using solely automated means. AI tools (notably Anthropic's Claude API) are used to *assist* drafting and triage of correspondence, under human-in-the-loop oversight. See the separate **AI Policy** for detail.

10. Children's data

Our services are directed at businesses and adults. We do not knowingly collect personal data of children under 13. If you believe a child's data has been submitted to us, contact us and we will delete it.

11. Changes to this policy

We will update this policy when our processing or processor list materially changes. The current version is dated at the top of this document; previous versions are available on request.
