97c Alexandra Road
Tipton
West Midlands
DY4 8TD
0121 295 1925
info@keironcheesbrough.com
www.keironcheesbrough.com

Keiron Cheesbrough Ltd · Registered in England and Wales · Company no. 11885860 · VAT GB 318 9406 84

Privacy Policy

Version 5 · Valid from 4 October 2026

This privacy policy explains how we use personal data when you visit our website, enquire, open an account, buy or receive our services, complain, speak up, subscribe to a newsletter, apply to join us through a public form, or verify an engineer via a staff ID QR code. It is the public notice for anyone outside our workforce. It is not the staff privacy policy.

---

1. Who We Are (the Controller)

For UK data protection law, the controller is:

Keiron Cheesbrough Ltd

Company number: 11885860 Registered office: 97c Alexandra Road, Tipton, West Midlands, DY4 8TD, United Kingdom VAT: GB 318 9406 84
ICO registration: ZB888956 Telephone: 0121 295 1925 Website: https://www.keironcheesbrough.com

Managing Director / owner: Keiron Cheesbrough

Data Protection Manager

Post: Data Protection Manager, Keiron Cheesbrough Ltd, 97c Alexandra Road, Tipton, West Midlands, DY4 8TD, United Kingdom Email: info@keironcheesbrough.com

We design, install, commission and maintain professional telecoms and security systems for customers across the UK.

---

2. Whose Data This Notice Covers

This notice applies to personal data about:

- customers and people who enquire about work
- account holders on our website

- people who contact us by phone, email or form
- complainants using our complaints process
- whistleblowers / people who use Speak up (named or anonymous)
- newsletter subscribers
- job and apprenticeship applicants who use public careers / join-team forms
- people who scan or open a public engineer ID verify page (`/id/…`)

It does **not** replace our internal staff privacy policy , which covers employees, workers and contractors engaged as workforce.

---

3. What We Collect and Where It Comes From

3.1 Information You Give Us

You may provide information by filling in website forms or by corresponding with us. Forms and channels include:

Source	Typical data
Contact / enquiry forms	Name, contact details, message, site address if given
Account registration	Name, email, phone, address, account preferences
Newsletter signup	Name/email (and confirmation of subscription)
Careers / join-team forms	Name, contact details, interest (job or apprenticeship), experience, qualifications, education, driving and availability you choose to give
Complaints form	Name, address, contact details preferred contact method, complaint details, desired outcome, optional extra-support information
Whistleblowing / Speak up	Report content; name/contact only if you choose to give them
Site feedback (website modal)	Name, email, message, and the page you were on — for product/UX feedback only (not an official complaint, and not a job review)
Job feedback after a visit	Star rating and optional written review of the work
Phone and email	Whatever you tell us so we can help
Quotes, jobs and account use	Site contacts, access notes, photos or plans you upload, payment and invoice details

Source	Typical data
Payments	Payment is handled by our payment processor (Stripe). We do **not** store full card numbers

We do not add customer or staff email addresses to the newsletter unless that person has subscribed and confirmed (double opt-in).

On the join-the-team form we do **not** ask for date of birth, National Insurance number or health information. If you choose to tick that you already hold vetting (for example DBS, NPPV3 or SC), we treat that as information you volunteered about qualifications you hold — we use it only to contact you about suitable work, not to run a check at that stage.

3.2 Information We Create or Receive in the Course of Work

- Job and account records (quotes accepted, appointments, invoices, engineer notes)
- Photos or files you upload so we can quote or do the job
- Service messages and logs linked to your account or job
- Job feedback: star ratings and written reviews after a visit
- First-party website analytics (see cookies section)

3.3 CCTV and Security Installs (Important)

When we survey, quote, install or maintain CCTV or other security systems at a customer site, we process **site contact and job data** (names, phones, emails, addresses, access instructions, photos of the installation) so we can do the work safely and keep a proper job record.

Camera Footage

recorded on equipment we install at a customer site is typically processed on **the customer's system**. Unless we have expressly agreed in writing to host, store or monitor footage for you, **that footage is the customer's responsibility** as controller of their own CCTV. We may view live or recorded images on site only as needed to install, commission, fault-find or demonstrate the system. If we ever host or monitor footage under a separate agreement, we will explain that processing at the time.

3.4 Extra-Support Information on Complaints (Special Category)

Our official complaints form lets you optionally tell us about extra support needs at the address (for example disability or limited mobility, hearing or sight, mental health or anxiety, older person, young children, language needs, or living alone). That information can be **special category** personal

data.

We only use it to acknowledge the complaint, investigate safely, visit safely if needed, and reply with the outcome. We do **not** use it for marketing. Access is limited to people who need it to handle that complaint. The additional condition we rely on under UK GDPR Article 9 / the Data Protection Act 2018 is typically that processing is necessary for the establishment, exercise or defence of legal claims, or another Schedule 1 condition that fits the support need you told us about. Extra-support details are optional. Prefer-not-to-say is available.

3.5 Public Engineer ID Cards (Digital ID via QR)

Our engineers may carry a physical ID card. The **back** of the card has a QR code that opens a unique **digital ID** page on our website (`/id/…`). Scanning it lets a customer or site verify the person in front of them.

That page shows limited ID details only: name, role or job title, whether the card is valid, and a photo when the card is valid. It does **not** show email, phone, home address, National Insurance number, certificate files, or a full training / clearance profile.

Training is separate. Training and clearance details are not published on the digital ID page and are not encoded in the card QR. We do not put training share links on the physical card.

Where appropriate, the verify page may let someone **request access** to that person's training profile. The request goes to the staff member and their manager; **either may approve**. If approved, we send a **signed, time-limited** training share link (same mechanism as today's admin training share — it expires). Until then, training stays private.

Each card has its own durable link (not a browsable staff directory). Those pages are kept out of search engines (`noindex` / robots rules). We use this so customers and sites can verify the engineer.

---

4. Purposes and Lawful Bases

We only use personal data when we have a lawful basis under UK GDPR. Typical purposes and bases:

Purpose	Lawful basis (typical)
Respond to an enquiry; provide a quote; take steps before a contract	Contract (pre-contract steps) and/or legitimate interests

Purpose	Lawful basis (typical)
Perform a contract for products or services; manage the account and job	Contract
Send service messages (survey times, appointment reminders, engineer arrival, invoices, payment follow-ups)	Contract and/or legitimate interests. These are **not** marketing. Automated or recorded calls for service are covered in our Website use policy (https://www.keironcheesbrough.com/terms)
Process payments via Stripe; keep accounting records	Contract; legal obligation
Handle complaints and keep them with the job file	Legitimate interests; legal obligation where applicable. Optional extra-support details: see section 3.4 (Article 9 condition)
Site feedback modal	Legitimate interests (improve the website and fix problems). Not an official complaint, and not a job review
Keep job feedback (star ratings and written reviews) for quality history	Legitimate interests
Investigate whistleblowing / Speak up reports	Legitimate interests; legal obligation where applicable
Newsletter and other marketing emails/texts	**Consent** (subscribe and confirm / double opt-in). You can withdraw at any time
Existing-customer offers for similar products or services (for example contacting a customer about an alarm service contract after an install)	**Legitimate interests**, and only where electronic marketing / phone rules (PECR) allow. Similar products/services to what you already had from us; easy opt-out; not cold calls to non-customers. Live marketing calls to individuals are screened against the Telephone Preference Service where required
Improve the website (first-party analytics); outdated-browser notice	Legitimate interests
Public engineer digital ID verify page (`/id/…`) via QR on staff ID cards	Legitimate interests (site security; preventing impersonation)

Purpose	Lawful basis (typical)
Training-profile access requests from the ID verify page; approved time-limited training share	Legitimate interests (site verification / demonstrating competence), with approval and link expiry
Consider join-team / careers applications	Consent (join-team form); legitimate interests / steps toward contract for a specific vacancy
Debt recovery where an account is overdue and the contract allows it	Legitimate interests; contract
Comply with law, regulators or lawful requests from police	Legal obligation / public interest as applicable
Defend legal claims; keep records for limitation periods	Legitimate interests; legal obligation

Marketing vs service messages: These are different.

- **Service messages** about an enquiry, account or job (appointments, engineer arrival, invoices, payment follow-ups) are not marketing. Automated or recorded calls for those purposes are covered in the Website use policy (https://www.keironcheesbrough.com/terms).
- **Newsletters and promotional emails/texts** only go out with **consent** and double opt-in for email. You can turn marketing texts off in your account and unsubscribe from emails using the link in each message, or contact us.
- **Existing-customer offers** for similar products or services (for example calling or emailing a past alarm-install customer about a maintenance / service contract) may rely on **legitimate interests**, and only where PECR allows. Limited to people who already had a relevant relationship with us, similar products/services, and an easy way to say no. Opt out anytime via info@keironcheesbrough.com, 0121 295 1925, or when we contact you.

You can withdraw newsletter/promotional **consent** at any time by using the unsubscribe link, turning texts off in your account, emailing info@keironcheesbrough.com, or phoning 0121 295 1925. Withdrawal does not affect processing already carried out lawfully.

---

5. Cookies and First-Party Analytics

We use **first-party analytics** on this website so we can see which browsers and pages are used, and so we can warn people on browsers that are no longer supported. Hits are recorded on **our servers**. This analytics does **not** set a cookie.

We record:

- browser family and version
- operating system (and version)
- device type (for example phone or desktop)
- the page path
- whether the visit looks like a bot, and whether the browser is one we still support
- whether you were a guest, a signed-in customer, or signed-in staff — we do **not** store your account id on the hit
- a daily technical identifier (a one-way hash of the date, browser and device, plus a one-way hash of your IP address with a **daily secret that we discard after that day**). We use this to count approximate unique browsers that day. Once the day's secret is gone, we cannot turn the identifier back into an IP address

We do **not** store IP addresses, advertising IDs, or a raw user-agent string for this analytics. We look at counts (pages, browsers, guests / customers / staff). We do not use it for advertising or to build a marketing profile.

Hits are kept for **90 days**, then deleted.

This processing is based on **legitimate interests** (see the table in section 4). You can **object** by contacting us (section 10). Because this analytics does not set a cookie, blocking cookies in your browser does not stop it.

If you dismiss the outdated-browser / unsupported-browser notice, we set a first-party cookie named `kc_browser_ok` with **Max-Age of 2,592,000 seconds (30 days)** so we do not show that notice again on this browser. It is only for that banner — not a general consent cookie.

The website also uses **strictly necessary** cookies so the site works securely — typically a session cookie and a CSRF protection token (for example `laravel_session` and `XSRF-TOKEN`). These are not used for advertising. If you use **Remember me** on login, your signed-in session may last longer (about 90 days) so you do not have to sign in every visit.

The website may register a **service worker** (`/sw`) so static assets load faster and so we can show optional notifications if your browser allows them. It caches technical assets on your device; it is not used for advertising.

This section is the cookie notice for our website. There is no separate cookie policy page. The Website use policy (https://www.keironcheesbrough.com/terms) points here for cookies and personal data.

---

6. Sharing and Processors

We do not sell your personal data. We share it only where needed to deliver a service, run the business lawfully, or where the law requires it.

Typical categories of recipients:

Category	Why
Couriers / logistics	Delivery of goods
Payment processor (Stripe)	Card and online payments — we do not store full card numbers
Email provider (one.com)	Outbound email, including service and (where consented) marketing messages
Phone / SMS provider (Twilio)	Calls, texts, and related telephony for service and (where allowed) marketing
Trusted IT / hosting and support providers under contract	Secure operation of our systems and website
Map / address lookup providers (Google or Nominatim, per Settings)	When a form offers address autocomplete, your browser talks only to **our** website; we then query the configured map provider to suggest matches. Only the lookup text (and related place ids) needed for suggestions is processed
UK postcode enrichment (postcodes.io)	Used **on our servers** to enrich or validate site postcodes (not called directly from your browser)
Maps apps via outbound link (e.g. Google Maps)	When you choose “Open in Maps” (or similar), you leave our site; that provider’s own privacy terms apply. We do not embed live map tracking pixels for advertising
Debt recovery agents	Where an account is overdue and recovery is lawful under the contract
Payroll bureau (TaxAssist)	Staff pay. The payroll file contains name, National Insurance number, hours, and holiday and sick days
Professional advisers (e.g. accountants, solicitors)	Where needed for advice or claims
Regulators, courts, police or other authorities	Where required or permitted by law

We use **trusted service providers under contract**. They may only process personal data on our instructions and with appropriate security. We do not invent or list every SaaS product name here; categories above describe the roles.

Address suggestions on the site go through our own geo endpoints to the map provider set in Settings (Google or Nominatim). Separately, we may use postcodes.io on our servers to enrich site postcodes. “Open in Maps” links are ordinary outbound links.

Manufacturer apps and cloud products we link to (for example Hik-Connect, ProControl+, Ring) have their **own** privacy terms. We do not control those products.

---

7. International Transfers

Personal data is processed primarily in the **United Kingdom** and, where relevant, the **EEA**.

Some trusted providers may process data outside the UK. Where that happens, we use appropriate safeguards required by UK data protection law (for example the UK International Data Transfer Agreement / Addendum, or an adequacy decision) so that your data remains protected.

If you need more detail about a specific transfer, contact the Data Protection Manager.

---

8. Retention

We keep personal data only as long as needed for the purpose, including legal and claim periods. Typical periods:

Category	Retention (typical)
Account / contract / job and invoice records	6 years after the end of the contract or account relationship (or longer if a claim is ongoing)
Complaints	Kept with the related job file for the same period as that file
Join-team / general careers interest form	12 months, then delete unless you join us or ask us to keep it
Specific vacancy applications (e.g. with CV)	**12 months**, then delete unless you join us or ask us to keep them (same as the join-the-team pool)
Newsletter	Until you unsubscribe (or we delete inactive records as good practice)
Website analytics	**90 days**, then deleted

Category	Retention (typical)
Whistleblowing / Speak up	As needed to investigate and take action, then in line with legal and claim needs
Site feedback (website modal only)	As needed to act on the feedback, then delete or anonymise; typically within 12 months unless linked to an ongoing issue. This is **not** job star ratings or written job reviews
Job feedback / star ratings / written reviews	Kept for quality history. We may retain these long-term, including for the life of the business. They are not deleted under the 12-month website-modal rule. If you ask us to erase your personal data, we remove or anonymise your name and contact on the review. We may keep the star score and an anonymised copy of the comment for stats and history where the law allows
Service call recordings (if used)	Call recordings are kept for 6 years, then deleted
Photos / plans you send for a quote or job	With the job / enquiry record as above
Payment records	As required for tax and accounting (typically with financial records for 6 years)

Shorter or longer periods may apply if the law requires it or if we need data for an active dispute or investigation.

---

9. Security

We take security seriously. Measures include password-protected and encrypted systems where appropriate, role-based access so staff only see what they need, and contracts with processors that require them to protect data. No method of transmission or storage is completely secure; we work to reduce risk to an appropriate level for the data we hold.

---

10. Your Rights

Under UK data protection law you can ask us to:

- **Access** your personal data (a subject access request)
- **Rectify** incomplete or inaccurate data

- **Erase** data where there is no good reason for us to keep processing it. For job feedback, that means we remove or anonymise your name and contact on the review; we may keep the star rating and an anonymised copy of the written review for quality history where the law allows
- **Restrict** processing in certain cases (for example while we check accuracy)
- **Object** to processing based on legitimate interests
- **Port** data you provided to us, where processing is based on consent or contract and is automated
- **Withdraw consent** where we rely on consent

We usually respond within **one month**. We may extend that by up to two further months for complex or numerous requests; if so we will tell you. We do not charge a fee in most cases, but we may charge a reasonable fee or refuse a request that is clearly unfounded, repetitive or excessive.

How to exercise your rights: email info@keironcheesbrough.com, call 0121 295 1925, or write to the Data Protection Manager at the registered office. We may need to verify your identity.

Marketing opt-out: unsubscribe link in emails; account settings for marketing texts; or contact us as above.

---

11. Children

You must be **18 or over** to create an account or to request work through our website (see Website use policy (https://www.keironcheesbrough.com/terms)). Someone 18 or over must be on site when we attend. We do not knowingly offer accounts to children.

---

12. Automated Calling for Service

If you enquire, hold an account, accept a quote or have a job with us, we may contact you about that work by email, text or phone. Some calls may be automated or recorded. They are used for reminders and scheduling — **not** for marketing. Full detail is in the Website use policy (https://www.keironcheesbrough.com/terms). You can ask us to stop automated calls at any time (email, phone or contact page).

---

13. Complaints

If you have a concern about how we use your data, please contact the Data Protection Manager first (details in section 1). We hope we can sort it out.

We are registered with the ICO (registration **ZB888956**).

You can also complain to the UK Information Commissioner's Office (ICO):

Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF Website: https://ico.org.uk

---

14. Changes to This Policy

We may update this notice. The version and dates shown with this page are the ones that apply. Material changes will be shown by updating the version and review dates. Check this page for the current text. A change here does not rewrite a quote you have already accepted.

---

15. Contact

Questions about this privacy notice: Email: info@keironcheesbrough.com Telephone: 0121 295 1925 Post: Data Protection Manager, Keiron Cheesbrough Ltd, 97c Alexandra Road, Tipton, West Midlands, DY4 8TD, United Kingdom