Privacy Policy

How We Use Your Information

The Cucumber Group

Version 2.3

Last updated: 20 March 2026

Next scheduled review: September 2026

The Cucumber Group ("we", "our", "us") is committed to protecting and respecting your privacy. This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you interact with us, including through our websites and services. Please read this policy carefully to understand our views and practices regarding your personal data and how we will treat it. This policy was last updated 20 March 2026.

1. Definitions

1.1. For the purposes of this Privacy Policy:

1.2. **The Cucumber Group** is a collective term for:

- **Cucumber Recruitment Ltd** (Company Registration Number: 11141112)
- **Cucumber Catering Ltd** (Company Registration Number: 11998440)
- **Cucumber Eco Solutions Ltd** (Company Registration Number: 11438494)
- **Cucumber Logistics Ltd** (Company Registration Number: 13385553)

All registered offices at: *Kimada House, 442 Flixton Road, Urmston, Manchester, M41 6QT.*

The term "Cucumber Group" is used solely as a collective style or brand name for ease of reference in public communications and internal policies. It does not represent a separate legal entity. The businesses associated with the Cucumber Group are four distinct and independent legal entities, each responsible for their own operations, obligations, and liabilities. Use of the Cucumber Group name does not imply a merger, joint venture, or shared legal responsibility among these entities.

1.3. **Personal Data** means any information relating to an identified or identifiable natural person.

1.4. **Special Category Data** means sensitive personal data as defined by UK GDPR Article 9, such as health information, racial or ethnic origin, and religious beliefs.

1.5. **Criminal Offence Data** means personal data relating to criminal convictions and offences as defined by UK GDPR Article 10, including DBS (Disclosure and Barring Service) and PVG (Protecting Vulnerable Groups) check data.

1.6. **Processing** means any operation performed on personal data, whether automated or not.

1.7. **Sensitive Data** means any personal data classified as special category under UK GDPR Article 9, or criminal offence data under Article 10 (e.g., DBS, PVG).

2. Information We Collect

2.1. Personal Data

We may collect and process the following personal data about you:

- **Identity Data:** Name, date of birth, gender, and identification documents.
- **Contact Data:** Address, email address, phone number.
- **Employment Data:** CVs, employment history, references, qualifications, and certifications.
- **Financial Data:** Bank account details, payment information.
- **Technical Data:** IP address, browser type, and version, time zone setting, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access this website.
- **Usage Data:** Information about how you use our website.
- **Marketing and Communications Data:** Your preferences in receiving marketing from us and your communication preferences.

2.2. Special Categories of Data

We may also collect and process special categories of personal data such as:

- Health information, including physical or mental health conditions, where relevant to job roles (especially in the healthcare sector).
- Criminal offence data, including DBS checks or disclosures where legally required for employment screening. Refer to Schedule 1 of this Policy "Schedule 1 — Criminal Record Declarations" for additional information.

3. How We Collect Your Data

We collect data through:

3.1. Direct Interactions

You may provide us with your data by:

- Applying for roles or registering with us.
- Booking staff via contact request forms.
- Filling in forms on our website.

- Communicating with us via post, phone, email, or otherwise.
- Requesting marketing or information.
- Participating in surveys or feedback processes.
- **Interacting with our AI assistants via WhatsApp or email** (see Section 5 for full details).

3.2. Automated Technologies

When you use our website, we may automatically collect Technical Data using:

- Cookies.
- Server logs.
- Other similar technologies.

For details on the cookies we use, please refer to our Cookie Policy, which can be found via our website.

4. How We Use Your Data

4.1. We use your personal data lawfully and fairly for the following purposes:

- **To perform our contract with you:** e.g., processing applications, matching to jobs, onboarding, and payroll.
- **To comply with legal obligations:** e.g., verifying identity, right to work checks, DBS reporting and HMRC reporting.
- **For our legitimate interests:** e.g., to run our business, improve services, protect IT systems, and conduct AI-assisted recruitment screening (see Section 5 below).
- **With your consent:** e.g., for specific marketing communications or processing sensitive data not required by law.

5. Use of AI and Automated Tools

5.1. Overview

We use artificial intelligence (AI) tools to support our recruitment and business operations. This section explains how we use AI, what data it may process, and what your rights are in relation to automated processing.

5.2. How We Use AI

We may use AI-powered tools to assist with:

- Screening candidates and matching them to roles based on experience, qualifications, and availability.
- Conducting initial candidate assessments via automated conversations (e.g. WhatsApp or email).
- Generating operational reports and managing recruitment workflows.
- Querying our recruitment database to support our team.
- Other recruitment and business support tasks.

5.3. Candidate-Facing AI

We may invite you to interact with an AI assistant as part of the recruitment process — for example, to conduct an initial screening conversation. In compliance with the Data (Use and Access) Act 2025, we will always tell you that you are communicating with an AI system, not a human. This disclosure is made at two points: in the screening invitation email and at the start of the AI conversation itself.

> **What the AI assessment involves:** Our AI assistant evaluates your suitability for a role based on your stated experience, qualifications, availability, and compliance status (such as right to work and DBS). This constitutes **profiling** under UK GDPR Article 4(4) — the automated processing of personal data to evaluate certain personal aspects. However, the AI does not make any decisions about your application. All AI-generated assessments are reviewed by a human recruiter before any recruitment decision is made (see Section 5.5).

During an AI-assisted conversation, you may be asked about:

- Your name and contact details
- Your work history and relevant experience
- Your availability and preferred working patterns
- Your location and willingness to travel
- Your right to work in the UK
- Your DBS (Disclosure and Barring Service) status
- Your healthcare qualifications and training

Special category data (Article 9): Healthcare qualifications are classified as special category data under UK GDPR Article 9. We only collect this information where it is required for the role you have

applied for, and **we will ask for your explicit consent before collecting it.**

Criminal offence data (Article 10): DBS status constitutes criminal offence data under UK GDPR Article 10. We process this data where it is necessary for compliance with employment law obligations and for safeguarding purposes, in accordance with DPA 2018 Schedule 1 (see Schedule 1 of this policy).

You can decline to provide special category or criminal offence data to the AI assistant and speak to a human recruiter instead, with no impact on your application.

5.4. How AI Providers Process Your Data

Our AI tools are powered by third-party AI providers who process your data on our behalf as data processors. Our current AI provider is:

- **Anthropic PBC** (provider of the Claude AI model) — a US-based company

Sending personal data to Anthropic's infrastructure constitutes an **international transfer** of personal data outside the United Kingdom under UK GDPR Chapter V. This transfer is governed by the **UK International Data Transfer Addendum** (UK IDTA) to the EU Standard Contractual Clauses, as issued by the ICO under Section 119A(1) of the Data Protection Act 2018.

Anthropic does not use your data to train its AI models. Your data is not retained by Anthropic beyond the active processing session. All data is transmitted securely using industry-standard encryption (TLS 1.2+).

If we change AI provider in future, this policy will be updated to reflect the new provider. The same safeguards and standards will apply.

5.5. Human Oversight

Automated tools do not make final decisions. All recruitment outcomes are subject to human review and final decision-making. A real person always reviews your application before any decision is made about progressing, shortlisting, or declining your candidacy. You will never be rejected solely on the basis of an AI assessment.

You have the right to:

- **Request human intervention** at any stage — you can ask to speak to a human recruiter instead of interacting with an AI assistant, with no negative impact on your application.
- **Challenge any decision** made with the help of automated processing — contact us using the details in Section 13 and a human recruiter will review your application.

5.6. AI Fairness and Monitoring

We regularly assess our AI tools to ensure accuracy and relevance, fairness, non-discrimination, transparency, and compliance with data protection laws. We periodically review AI screening outcomes for patterns that may suggest bias against any protected characteristic.

6. Lawful Basis for Processing

6.1. We rely on the following lawful bases under the UK GDPR:

- **Contract** — to fulfil our obligations to you (e.g. job placement, payroll).
- **Legal obligation** — where required by law (e.g. right to work, DBS checks).
- **Legitimate interests** — for efficient recruitment, client services, and business operations, including the use of AI tools for screening and matching. We conduct assessments to ensure these do not override your rights.
- **Consent** — where required (e.g. for certain special category data collected via AI screening, or for marketing).

You can object to processing based on legitimate interests at any time.

Specific to AI screening:

- **Special category data** (healthcare qualifications): We rely on your **explicit consent** (UK GDPR Article 9(2)(a)). You can withdraw your consent at any time by contacting us using the details in Section 13. In certain circumstances, processing may also be lawful under Article 9(2)(b) (necessary for employment law obligations) or Article 9(2)(g) (substantial public interest), for example where healthcare qualifications are required by regulation for the role.
- **Criminal offence data** (DBS status): We rely on **DPA 2018 Schedule 1, Parts 1 and 2** — processing is necessary for compliance with employment law obligations and for safeguarding purposes. This is governed by UK GDPR Article 10, which is distinct from the special category data provisions of Article 9. See Schedule 1 of this policy for full details.

7. How We Share Your Data

7.1. We may share personal data with local authorities, the police, social services, and other safeguarding bodies where necessary to protect a child or vulnerable adult(s). Such disclosures are made under the lawful bases of:

7.1.1. Article 6(1)(c) UK GDPR — compliance with a legal obligation (including duties under the Children Act 1989, Children Act 2004, and Care Act 2014), and

7.1.2. Article 6(1)(e) UK GDPR — performance of a task carried out in the public interest, specifically safeguarding.

7.2. Where the circumstances require it, we may also rely on Article 6(1)(d) — vital interests (protecting life or serious harm).

7.3. We will always share the minimum amount of information necessary and maintain a record of any safeguarding disclosures made.

7.4. In addition to the disclosures that may be made in accordance with clause 7.1., we may also disclose your data to:

- Clients and potential employers for recruitment opportunities.
- Third-party service providers for IT systems, cloud storage, background checks, payroll, etc.
- **AI service providers** who process data on our behalf (see Section 5.4).
- Professional advisers such as lawyers, accountants, and insurers.
- Regulatory authorities such as the HMRC or DBS where legally required.

7.5. Transfer Outside of the UK/EEA

- In certain circumstances, personal data may be processed or accessed outside the UK/EEA. For example, our operations team in South Africa may access limited personal data to facilitate recruitment, bookings, and client services.
- Such transfers are strictly controlled, with appropriate safeguards in place, including:
    - The **UK International Data Transfer Addendum** (UK IDTA) to the EU Standard Contractual Clauses, as issued by the ICO under Section 119A(1) of the Data Protection Act 2018.
    - Encryption of data in transit.
    - Access limited to authorized personnel bound by confidentiality obligations.
- No sensitive data, including DBS or PVG information, is transferred outside the UK/EEA unless absolutely necessary and safeguarded as above.
- All personal data transferred outside the UK/EEA, including to our operations team in South Africa, is encrypted in transit and stored securely in accordance with our Data Security measures in Clause 8.

All third parties must comply with data protection laws and only process your data under our instructions.

8. Data Security

8.1. We implement appropriate technical and organizational measures to protect your personal data, including:

- **Encryption** of personal and sensitive data both at rest (stored on our servers or databases) and in transit (during transfer over networks).
- Use of **secure servers** with restricted access to authorized personnel only.
- Staff training and **confidentiality agreements** to safeguard personal data.
- Regular system monitoring, **penetration testing**, and audit logging for highly sensitive information such as DBS or PVG records.
- Access permissions and technical safeguards are reviewed regularly, and penetration testing is conducted at least annually to ensure security and compliance with UK GDPR requirements.
- **AI-specific security measures:** Role-based access controls for AI tools, whitelist-based access to AI systems, monthly access reviews, automated security monitoring, and disappearing messages to limit data persistence on devices.

9. Data Retention

9.1. We retain your personal data only as long as necessary for the purposes set out above. The retention periods below reflect the different categories of data we process:

Data Category	Retention Period	Deletion Method
Standard personal data (CV, contact details, employment history)	12 months from last active engagement, unless you request deletion earlier	Secure deletion from CRM
AI screening conversations	12 months from screening date	Automated deletion from platform
AI-generated assessment summaries	12 months from screening date	Secure deletion alongside conversation data
DBS certificates (full copies)	12 months from date of issue	Secure destruction (see Schedule 1)

Data Category	Retention Period	Deletion Method
DBS summary records (reference number, date, outcome)	Duration of engagement + 12 months	Secure deletion from CRM
Healthcare qualification records	Duration of engagement + 12 months	Secure deletion from CRM
CRM query logs (internal AI tool usage)	12 months rolling	Automated log rotation

9.2. Longer retention may apply where required for legal, tax, or regulatory reasons. We may anonymise data for statistical purposes, in which case it is no longer considered personal data.

9.3. **AI providers:** Our AI provider (Anthropic) does not retain your data beyond the active processing session. Data transmitted to Anthropic is ephemeral and is not stored after the interaction ends.

10. Your Legal Rights

10.1. **You have rights under UK data protection law, including the right to:**

- Request access to your data.
- Request correction of inaccurate data.
- Request erasure ("right to be forgotten").
- Object to processing (especially profiling or marketing).
- Request restriction of processing.
- Request data portability (in applicable cases).
- Withdraw consent at any time (where consent is the basis).
- **Request human intervention** in any AI-assisted decision (see Section 5.5).
- **Challenge any decision** made with the help of automated processing (see Section 5.5).
- **Opt out of AI screening** and request to interact with a human recruiter instead, with no negative impact on your application.

To exercise your rights, contact us using the details below.

Requests will be processed within one month of receipt, in accordance with UK GDPR.

11. Data Controller(s)

11.1. Each entity within the Cucumber Group is a data controller, responsible for its own processing activities under UK GDPR:

- **Cucumber Recruitment Ltd** — healthcare recruitment and placements, including internal hiring/HR.
- **Cucumber Catering Ltd** — catering staff recruitment and placement, including internal hiring/HR.
- **Cucumber Eco Solutions Ltd** — environmental projects, customer data through submissions and referrals, and internal hiring/HR (does not undertake recruitment of external candidates).
- **Cucumber Logistics Ltd** — logistics staff recruitment, placement and operations including internal hiring/HR.

11.2. Each entity determines the purposes and means of processing for its own data.

11.3. The Data Protection Officer coordinates Group-wide privacy governance but does not act as sole data controller.

12. Changes to this Privacy Policy

12.1. We may update this policy from time to time. Changes will be posted on this page and dated, and, where appropriate, notified by email. Please check this page periodically to stay informed.

12.2. **Next scheduled review:** September 2026 (6-month review cycle).

13. Contact Information

For privacy-related queries, or if you have any questions about this Privacy Policy or our use of your data, please contact:

Giordano Baseggio — Data Protection Officer (acting across Cucumber Group entities)
Kimada House, 442 Flixton Road, Urmston, Manchester, M41 6QT.
Email: giordano.baseggio@cucumber-recruitment.com
Phone: 0161 509 6097

You also have the right to complain to the Information Commissioner's Office (ICO): www.ico.org.uk

Schedule 1 — Criminal Record Declarations

1. Purpose

1.1. This Schedule sets out how The Cucumber Group processes information relating to criminal record checks, including but not limited to DBS (Disclosure and Barring Service) checks, Disclosure Scotland checks, and PVG (Protecting Vulnerable Groups) Scheme membership.

1.2. Processing of such data is necessary to meet our legal, contractual, and safeguarding obligations.

2. Collection of Criminal Record Information

2.1. Criminal record information will only be requested and processed where it is both relevant and proportionate to the role being applied for or undertaken.

2.2. Individuals will be informed at the point of collection why the check is required and how the data will be used.

3. Retention of Certificates

3.1. Copies of DBS and PVG disclosure certificates will be retained for a maximum of twelve (12) months from the date of issue. This extended retention is documented in the Group's Appropriate Policy Document and is subject to strict access and security controls.

3.2. At the end of the twelve (12) month period, certificates will be securely destroyed in accordance with The Cucumber Group's data security procedures.

4. Retention of Summary Records

4.1. Following the destruction of certificates, The Cucumber Group will retain a **summary record** for compliance, safeguarding, and audit purposes.

4.2. The summary record may include the following information:

- Disclosure reference number.
- Date of issue.
- PVG Scheme membership number and date (where applicable).
- Disclosure Scotland reference (where applicable).
- Confirmation of convictions, or confirmation that none were recorded.

- Details of any DBS Update Service checks conducted.
- The decision made regarding employment or engagement suitability.

5. Security and Access

5.1. Access to criminal record data, whether full certificates (during the retention period) or summary records, will be strictly limited to authorized personnel with a legitimate need to know.

5.2. Appropriate technical and organizational measures will be in place to ensure confidentiality, integrity, and security of such data.

6. Individual Rights

6.1. Individuals retain their rights under data protection law in respect of criminal record data, including the right to access, rectify, or request erasure, subject to legal and safeguarding requirements.

6.2. Any requests to exercise these rights should be submitted in writing to the Data Protection Officer as specified in this policy in clause 13.