Privacy Policy – How We Use Your Information

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 19 November 2025.

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 such as health information or criminal offence data.

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

1.6. **Sensitive Data** means any personal data classified as special category under UK GDPR, including health information and criminal offence data (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.

3.2. Automated Technologies

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

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

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-based CV screening (see 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. We may use automated tools, including artificial intelligence (AI), to support our recruitment process. This includes:

- Screening CVs and matching candidates to roles based on keywords, experience, and qualifications.
- Scoring or ranking applications to support shortlisting.

Important: Automated tools *do not* make final decisions. All recruitment outcomes are subject to human review and final decision-making. You have the right to request human intervention and challenge any decision made with the help of automated processing.

We regularly assess our AI tools to ensure accuracy and relevance, fairness, non-discrimination, transparency, and compliance with data protection laws.

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. We conduct assessments to ensure these do not override your rights.
- Consent – where required (e.g. for certain special category data, or for marketing).

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

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.
- 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 onboarding team in South Africa may access limited personal data to facilitate recruitment and client services.

- Such transfers are strictly controlled, with appropriate safeguards in place, including:

  - Standard Contractual Clauses (SCCs) approved under UK GDPR.
  - 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 onboarding 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.

9. Data Retention

9.1. We retain your personal data only as long as necessary for the purposes set out above, including:

- Usually, 12 months from your last active engagement with us (unless you request deletion earlier).
- Longer where required for legal, tax, or regulatory reasons.
- We may anonymize data for statistical purposes, in which case it is no longer considered personal data.

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).
- 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 Legal & Compliance Manager 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.

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 – Legal & Compliance Manager (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 Legal & Compliance Manager as specified in this policy in clause 13.