Data Protection Policy

Issued by: Clarence Recruitment ("the Company")
Date: August 2026
Review Cycle: Annual, or sooner where required

1. Purpose

Clarence Recruitment is committed to protecting the privacy and security of personal information entrusted to us.

As a recruitment business, we collect and process personal data relating to candidates, temporary workers, clients, employees, suppliers and other individuals. Some of the information we process may include **special category data**, such as information relating to health, ethnicity or other protected characteristics, where there is a lawful and appropriate reason for doing so.

Clarence Recruitment will comply with all applicable UK data protection legislation, including the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018,** together with any subsequent legislation or regulatory requirements that apply to our processing of personal data.

This policy explains how Clarence Recruitment manages personal data and the responsibilities of employees and contractors when handling personal information.

It should be read alongside the Company's **Data Protection Procedure, Privacy Notices, Information Security Policy and Data Retention Policy.**

2. Scope

This policy applies to all employees, directors, contractors and other individuals acting on behalf of Clarence Recruitment who have access to or process personal data.

It applies to personal data held in any format, including:

- electronic records and databases;
- emails and electronic communications;
- recruitment and candidate management systems;
- payroll and financial systems;
- paper records and documents;
- CVs and application information;
- identification and compliance documentation; and
- information provided by clients, candidates, temporary workers or third parties.

All individuals working for or on behalf of Clarence Recruitment are responsible for following this policy and reporting any concerns or suspected breaches promptly.

3. Definitions

For the purposes of this policy:

Personal data means information relating to an identified or identifiable living individual. This may include names, contact details, identification information, employment history, financial information, online identifiers and other information relating to an individual.

Special category data means personal data that is considered particularly sensitive under data protection law. This includes information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, health, and sex life or sexual orientation.

Data subject means the individual to whom personal data relates.

Processing means anything that is done with personal data, including collecting, recording, storing, accessing, using, sharing, amending or deleting it.

Data controller means the organisation that determines why and how personal data is processed.

Data processor means an organisation that processes personal data on behalf of a data controller.

Personal data breach means a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Consent means a freely given, specific, informed and unambiguous indication that an individual agrees to the processing of their personal data for a particular purpose.

4. Clarence Recruitment's Role

Clarence Recruitment will generally act as a **data controller** when processing personal data for its own recruitment, employment, business administration, marketing, compliance and operational purposes.

Where Clarence Recruitment processes personal data on behalf of a client or another organisation, it may act as a **data processor.** In these circumstances, Clarence Recruitment will comply with the relevant contractual and legal requirements governing that processing.

Where third-party organisations process personal data on behalf of Clarence Recruitment, we will take appropriate steps to ensure that they provide suitable safeguards and process personal data only in accordance with our instructions and applicable data protection law.

5. Personal Data We Process

Depending on the nature of our relationship with an individual, Clarence Recruitment may process information including:

- name and contact details;
- date of birth and identification information;

- employment history and qualifications;
- CVs, references and application information;
- right-to-work and identity verification information;
- professional registrations and certifications;
- DBS and other compliance information where applicable;
- availability and work preferences;
- payroll and payment information;
- bank details;
- tax and National Insurance information;
- attendance, timesheet and booking information;
- information relating to performance or conduct;
- correspondence and communications;
- photographs where appropriate and lawfully obtained;
- information relating to health or disability where necessary for recruitment, employment, workplace adjustments or compliance purposes; and
- other information necessary to provide recruitment and work-finding services.

We will only collect and process information that is necessary, relevant and proportionate to the purpose for which it is being used.

6. Purposes for Processing Personal Data

Clarence Recruitment may process personal data for the following purposes:

- providing recruitment and work-finding services;
- registering and managing candidates and temporary workers;
- identifying suitable employment opportunities;
- introducing candidates to clients;
- carrying out recruitment and selection activities;
- completing identity, right-to-work and compliance checks;
- obtaining and verifying references;
- managing bookings, placements and assignments;
- administering payroll and payments;
- managing client relationships;
- communicating with candidates, clients and other stakeholders;
- managing employee records and HR administration;
- financial and accounting administration;
- marketing and business development;
- maintaining business records;
- managing complaints, disputes and legal claims;
- complying with legal, regulatory and contractual obligations;
- preventing fraud and other unlawful activity;
- managing information security and business continuity; and
- any other legitimate purpose communicated to the relevant individual.

7. Data Protection Principles

Clarence Recruitment will ensure that personal data is:

- **Processed lawfully, fairly and transparently.**
- **Collected for specified, explicit and legitimate purposes** and not subsequently used in a way that is incompatible with those purposes.
- **Adequate, relevant and limited to what is necessary** for the purposes for which it is processed.
- **Accurate and kept up to date** where necessary.
- **Not retained for longer than necessary** for the relevant purpose or legal obligation.
- **Processed securely,** using appropriate technical and organisational measures to protect it against unauthorised or unlawful processing, accidental loss, destruction or damage.
- **Accountable,** meaning Clarence Recruitment must be able to demonstrate compliance with these principles.

8. Lawful Basis for Processing

Clarence Recruitment will only process personal data where there is a lawful basis for doing so.

Depending on the circumstances, this may include:

- **Consent** – where an individual has given clear and informed consent for their data to be processed for a specific purpose.
- **Contract** – where processing is necessary to enter into or perform a contract.
- **Legal obligation** – where processing is necessary for Clarence Recruitment to comply with a legal requirement.
- **Vital interests** – where processing is necessary to protect someone's life.
- **Public task** – where processing is necessary for a task carried out in the public interest or under official authority.
- **Legitimate interests** – where processing is necessary for a legitimate business interest, provided that this is not overridden by the individual's rights and interests.

Consent will not be used where another more appropriate lawful basis applies.
Where special category data is processed, Clarence Recruitment will also identify and document an appropriate additional condition for processing in accordance with data protection legislation.

9. Special Category Data

Because of the nature of recruitment and education recruitment, Clarence Recruitment may occasionally process special category data, including information relating to health, disability, ethnicity or other sensitive information.

Such information will only be collected and processed where there is a lawful basis and an appropriate additional condition under data protection legislation.

Access to special category data will be restricted to individuals who have a legitimate business need to access it.

Staff must not request, record, disclose or share special category data unless there is a clear and lawful reason for doing so.

10. Privacy Notices

Clarence Recruitment will provide appropriate privacy information to individuals explaining:

- what personal data we collect;
- why we collect it;
- how we use it;
- the lawful basis for processing;
- who we may share it with;
- how long we expect to retain it;
- the individual's rights;
- how to contact us about data protection matters; and
- how to complain to the Information Commissioner's Office (ICO).

Where personal data is obtained from a third party rather than directly from the individual, Clarence Recruitment will provide the required privacy information in accordance with applicable legislation.

11. Individual Rights

Individuals have a number of rights under data protection legislation. Depending on the circumstances, these include the right to:

- be informed about how their personal data is used;
- access their personal data;
- request correction of inaccurate or incomplete data;
- request erasure of their personal data;
- request restriction of processing;
- object to certain types of processing, including direct marketing;
- request data portability in applicable circumstances; and
- have certain safeguards applied where decisions are made solely by automated means and have a legal or similarly significant effect.

These rights are subject to certain legal exceptions and are not absolute in every circumstance.

12. Data Subject Requests

Any request from an individual exercising their data protection rights must be referred promptly to **Mia Jones, Head of Business Services & Governance,** at:
Email: mia@clarencerecruitment.co.uk

Staff should not respond substantively to a data subject request without first referring it to Mia or the person responsible for data protection within the Company.

Clarence Recruitment will normally respond to valid requests within **one month** of receipt. Where permitted by law, this period may be extended where a request is complex or where an individual has made multiple requests.

We may request additional information to verify an individual's identity before responding to a request.

13. Data Accuracy

Clarence Recruitment will take reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date.

Individuals should notify us if their personal information changes or if they believe information we hold about them is inaccurate.

Staff must also take reasonable care to ensure that information they enter into Company systems is accurate and complete.

14. Data Minimisation

Clarence Recruitment will only collect and retain personal data that is necessary, relevant and proportionate to the purpose for which it is required.

Staff should not collect or retain personal information simply because it may be useful in the future.

Where personal data is no longer required and there is no legal or legitimate reason for retaining it, it should be securely deleted or destroyed in accordance with the Company's data retention procedures.

15. Data Retention

Clarence Recruitment will retain personal data only for as long as it is necessary for the purpose for which it was collected, or where retention is required by law, regulation, contractual obligations or for the establishment, exercise or defence of legal claims.

Different categories of information may therefore be retained for different periods.

The Company will maintain appropriate retention periods and procedures for the secure deletion or destruction of information when it is no longer required.

16. Data Sharing and Third Parties

Clarence Recruitment may share personal data with third parties where there is a lawful basis for doing so.

- Depending on the circumstances, this may include:
- clients and prospective clients;
- schools, academies and education establishments;
- payroll providers;
- identity and right-to-work verification providers;
- DBS and other compliance providers;
- umbrella companies;

- software and technology providers;
- professional advisers;
- regulatory and government bodies;
- insurers;
- legal advisers; and
- other third parties where necessary to provide recruitment services or comply with legal obligations.

Before sharing personal data, Clarence Recruitment will ensure that there is a lawful basis for the disclosure and that only information necessary for the relevant purpose is shared.

Where appropriate, contractual arrangements and data processing agreements will be put in place with third-party providers.

17. International Transfers

Where personal data is transferred outside the UK, Clarence Recruitment will ensure that the transfer is made in accordance with applicable data protection legislation and that appropriate safeguards are in place.

18. Privacy by Design and Default

Data protection will be considered when introducing new systems, processes, services or ways of working that involve personal data.

Where appropriate, Clarence Recruitment will apply measures including:

- data minimisation;
- appropriate access controls;
- pseudonymisation or anonymisation where appropriate;
- encryption and other security measures;
- secure storage;
- appropriate retention and deletion procedures; and
- privacy impact assessments where required.

19. Information Security

Clarence Recruitment will implement appropriate technical and organisational measures to protect personal data.

Staff must:

- keep passwords and login details confidential;
- use Company-approved systems and software;
- not share personal data with unauthorised individuals;
- take care when sending emails containing personal data;
- use secure methods when transferring sensitive information;
- lock or secure devices when unattended;
- report lost or stolen devices immediately; and
- follow the Company's information security procedures.

Personal data must not be stored on personal devices or personal accounts unless specifically authorised by the Company.

20. Personal Data Breaches

A personal data breach may include:

- sending personal data to the wrong recipient;
- losing a laptop, phone or other device containing personal data;
- unauthorised access to a system;
- accidental disclosure of personal information;
- hacking or malware;
- loss or theft of paper records; or
- accidental deletion or destruction of personal data.

All suspected or actual data breaches must be reported **immediately** to:
Mia Jones – Head of Business Services & Governance
Email: mia@clarencerecruitment.co.uk

Staff must not attempt to conceal or independently resolve a suspected breach without reporting it. Clarence Recruitment will assess the breach and take appropriate steps to contain it, recover information where possible and prevent further loss or disclosure.

Where a breach is likely to result in a risk to individuals' rights and freedoms, the Company will notify the ICO within the applicable statutory timeframe. Where a breach is likely to result in a high risk to affected individuals, they will also be informed where required.

Where Clarence Recruitment is acting as a data processor, it will notify the relevant data controller without undue delay in accordance with the applicable contractual and legal requirements.

21. Complaints

If an individual has a concern about how Clarence Recruitment has handled their personal data, they should contact:

Mia Jones
Head of Business Services & Governance
Email: mia@clarencerecruitment.co.uk

Clarence Recruitment will investigate complaints fairly and promptly in accordance with its **Complaints Policy and Procedure.**

Individuals also have the right to complain directly to the **Information Commissioner's Office (ICO)** if they remain dissatisfied with how their personal data has been handled.

ICO website: Information Commissioner's Office

22. Staff Responsibilities

All employees and contractors are responsible for protecting personal data that they access or process as part of their role.

Staff must:

- comply with this policy and related procedures;
- only access information required for their role;
- keep personal data secure;
- maintain confidentiality;
- follow retention and deletion procedures;
- report inaccurate information where identified;
- report suspected data breaches immediately; and
- complete any data protection training required by the Company.

Failure to comply with this policy may result in disciplinary or contractual action.

23. Data Protection Responsibility

Mia Jones, Head of Business Services & Governance, is the Company's designated internal contact for data protection matters.

She is responsible for coordinating the Company's data protection compliance, including:

- responding to data subject requests;
- coordinating responses to data protection complaints;
- maintaining data protection policies and procedures;
- coordinating personal data breach investigations;
- monitoring compliance with data protection requirements;
- supporting staff with data protection queries; and
- liaising with the ICO and other relevant authorities where necessary.

This designation does **not** in itself mean that Mia Jones is formally appointed as the Company's statutory Data Protection Officer (DPO).

Clarence Recruitment will review periodically whether it is legally required to appoint a DPO and will make a formal appointment if required.

24. ICO Registration and Data Protection Fee

Where required by law, Clarence Recruitment will maintain its registration with the Information Commissioner's Office and pay the applicable data protection fee.

The Company will ensure that its registration details remain accurate and that the fee is renewed when required.

ICO Registration Reference: ZA394967

25. Review of this Policy

This policy will be reviewed annually, or sooner where there are changes to legislation, regulation, ICO guidance, Company systems or working practices.

The Company will update this policy where necessary to ensure that it continues to reflect Clarence Recruitment's data protection obligations and operational practices.
Policy Owner: Mia Jones, Head of Risk and Compliance
Next Review Date: August 2027