

GDPR & Data Protection Policy

Alvo recruitment

1. Purpose

This policy explains how Alvo recruitment collects, processes, stores, shares and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection legislation.

As a specialist health and social care recruitment agency, we are committed to protecting the privacy and rights of all individuals whose personal information we process.

2. Scope

This policy applies to:

Employees

Temporary workers

Job applicants

Candidates

Clients

Contractors

Suppliers

Website visitors

Any third party whose personal data is processed by the company

3. Data Controller

Alvo recruitment acts as the Data Controller for personal data collected during recruitment and business operations.

4. Information We Collect

We may collect and process:

Personal Information

Name

Address

Date of birth

Email address

Telephone number

National Insurance number

Right to work documentation

Passport details

Driving licence (where required)

Employment history

Qualifications

Professional registrations

References

Sensitive Personal Data (Special Category Data)

As a health and social care recruiter we may collect:

DBS information

Health information where necessary

Disability information

Occupational health information

Vaccination status where required by clients or legislation

Equality and diversity information (where appropriate)

Special category data is only processed where permitted under UK GDPR and relevant employment legislation.

5. Lawful Basis for Processing

We process personal information under one or more of the following lawful bases:

Consent

Performance of a contract

Legal obligation

Legitimate interests

Vital interests where appropriate

Special category data is processed under Article 9 UK GDPR where applicable.

6. Why We Process Personal Data

We process information to:

Recruit candidates

Match candidates with vacancies

Verify qualifications and registrations

Carry out right to work checks

Conduct DBS checks

Arrange interviews

Manage employment

Process payroll

Meet legal obligations

Comply with NHS, CQC and client requirements

Communicate with candidates and clients

Improve our recruitment services

7. Data Sharing

We only share information where necessary.

This may include:

NHS organisations

Care providers

Local authorities

Umbrella companies

Payroll providers

Pension providers

Disclosure and Barring Service (DBS)

Professional regulatory bodies

Occupational health providers

IT service providers

Government departments where legally required

We do not sell personal data.

8. International Transfers

Where personal information is transferred outside the UK, appropriate safeguards will be implemented in accordance with UK GDPR.

9. Data Security

We protect information by using:

Password-protected systems

Multi-factor authentication where available

Secure cloud storage

Encryption

Secure email practices

Staff confidentiality agreements

Access controls based on business need

Regular software updates

Anti-virus and cyber security measures

10. Data Retention

We retain personal data only for as long as necessary.

Typical retention periods include:

Recruitment records: up to 12 months where no placement is made (unless consent is obtained to retain them longer)

Worker records: normally six years after employment ends

Payroll records: six years

Right to work documentation: two years after employment ends

DBS information: only for as long as permitted by DBS guidance

Data is securely deleted or destroyed once no longer required.

11. Individual Rights

Individuals have the right to:

Access their personal information

Correct inaccurate information

Request deletion where applicable

Restrict processing

Object to processing

Request data portability

Withdraw consent where consent is relied upon

Lodge a complaint with the Information Commissioner's Office (ICO)

Requests should be made in writing to:

Email: nick@alvorecruitment.com

12. Subject Access Requests

Requests for personal information will normally be responded to within one calendar month in accordance with UK GDPR.

13. Data Breaches

All staff must report suspected personal data breaches immediately.

The company will:

Investigate the incident

Contain the breach

Assess risks

Notify affected individuals where required

Report notifiable breaches to the Information Commissioner's Office within 72 hours where legally required

Record all breaches internally

14. Staff Responsibilities

All employees must:

Handle personal data confidentially

Use company systems securely

Keep passwords confidential

Report breaches immediately

Complete data protection training

Follow company policies at all times

Failure to comply may result in disciplinary action.

15. Cookies and Website Data

Our website may collect information through cookies and analytics to improve user experience. Users can manage cookie preferences through their browser settings or our cookie banner.

16. CCTV

Where CCTV is used, recordings are retained only as long as necessary for security purposes and are accessed only by authorised personnel.

17. Policy Review

This policy will be reviewed annually or sooner if legislation changes or business operations require updates.