Desian Recruitment Ltd Record Retention Policy

This policy sets out how Desian Recruitment Ltd retains, stores, and securely disposes of records in line with legal, regulatory, and safeguarding obligations.
This applies to all records held by the organisation, including those relating to: Candidates, employees, contractors and clients, both electronic and paper records.

Principles

Only data necessary for business, legal, or safeguarding purposes will be retained.
Records will not be kept longer than necessary.
All retained data must be stored securely with appropriate access controls.
The organisation will maintain clear records of retention and disposal decisions.

Data Storage

Electronic Records

- Stored in secure, access-controlled systems
- Password protection and role-based access enforced
- Encryption used for sensitive/special category data

Physical Records

- Stored in locked cabinets or secure offices and access restricted to authorised personnel only.

Data Disposal

When retention periods expire, records must be securely destroyed:
Electronic Data to be permanently deleted from systems and removed from backups where feasible.
Paper Records to be cross-shredded or disposed via confidential waste services
Disposal Logs

- A record must be kept of:
- What was destroyed
- When
- By whom

Data Subject Rights

- Retention must comply with individual rights under UK GDPR, including:
- Right of access (Subject Access Requests)
- Right to rectification
- Right to erasure (where applicable)
- Right to restrict processing

These rights may be restricted where safeguarding or legal obligations apply.
Safeguarding obligations take precedence over standard retention periods.
This means that data may be retained longer where risk remains, information may be shared without consent if a child is at risk and those decisions must be documented and justified.

Retention Schedule

Recruitment & Candidate Records

- CVs (unsuccessful candidates): 6 months
- Interview notes: 6 months
- Candidate files (placed workers): 1 year after last assignment
- Right to Work documentation: duration of engagement + 2 years
- Vetting/compliance documents: 1–2 years after last placement

Employee Records

- Personnel files: 6 years after employment ends
- Contracts of employment: 6 years post-employment
- Disciplinary/grievance records: 6 years
- Payroll, PAYE, and tax records: 6 years
- Pension records: up to 6 years or longer where required

Safeguarding incident reports

- Minimum 6 years, longer if high risk

DBS checks:

- Do not retain certificates, just keep a record of check only (number, date, outcome).

Safeguarding records must be:

- Stored separately from general personnel files, with highly restricted access and transferred securely when required

Client Records

- Contracts and agreements: 6 years after termination
- Service delivery records: 6 years
- Client communications: 3–6 years

Complaints & Misconduct Records

- General complaints: 3–6 years
- Serious misconduct: 6 years minimum
- Safeguarding-related allegations: long-term or indefinite retention where justified

Financial Records

- Invoices, accounts, and tax records: 6 years minimum
- Audit records: 6 years

Data Protection Records

- Subject Access Requests (SARs): 3 years
- Data breach records: 6 years
- Consent records: duration of processing + 2 years

Always follow this policy and report any data risks or breaches immediately to management as non-compliance to this policy may result in disciplinary action, regulatory penalties or reputational damage.

Monitoring & Review

This policy is reviewed annually
Updates will be made in line with legal, regulatory, or operational changes.

Approved by: Andrew Wainwright
Position: Operations Director
Effective Date: 01/05/26
Next Review Date: 01/05/27