

Data Protection Policy

A1 Locums Ltd | Internal policy | Version 3, October 2026

1. Purpose and scope

A1 Locums is a veterinary recruitment and introduction agency. It introduces candidates to veterinary practices and corporate groups but does not employ or pay the locums it introduces. This policy covers personal information about candidates, locums, client contacts and A1 staff handled in its recruitment and business operations. It replaces the May 2018 policy when approved.

A1 complies with the UK GDPR, Data Protection Act 2018 and applicable data protection legislation. It provides clear privacy information to individuals and maintains appropriate records of processing.

2. Accountability and responsibilities

A1 is generally the controller of candidate registration, recruitment administration and pre-placement checking records. Practices will usually be separate controllers for their own engagement and statutory checks. TrustID describes itself as a processor when providing identity document checking services to its customers; the applicable contract and services must be checked.

The Managing Director, Clare Alderton, is responsible for overseeing A1 Locums' data protection compliance, supported by authorised recruiters and administrators.

All staff must report suspected data breaches and data protection requests promptly to Clare Alderton at info@a1locums.com.

3. Information we use and why

Recruitment	Names, contact details, CVs, qualifications, professional registrations, references, availability, preferences and booking history to provide work-finding and introduction services.
Identity and RTW	Identity documents, immigration status or online check outputs, verification results, dates, and necessary restrictions to help verify eligibility and manage relevant legal compliance.
Business records	Client contact details, booking details, fee records, correspondence and records needed for accounting, business administration and potential legal claims.
Additional information	Only where necessary and lawful: relevant special category information, criminal offence data or biometric identity-verification data. Such processing needs separate conditions and safeguards.

A1 records the correct UK GDPR Article 6 lawful basis for each activity in its processing record. Legitimate interests may support ordinary introduction and administration activities, contract may apply to services supplied to individuals or practices, and legal obligation applies only where the law imposes a duty on A1. Consent is not a universal basis for routine recruitment processing.

4. Digital identity checks and TrustID

A1 Locums uses TrustID to undertake digital Right to Work verification as part of its candidate registration process. In addition, A1 conducts a video call with each candidate to confirm that the individual matches the identity information provided.

TrustID may process identity documents, photographs and other personal information necessary to undertake the relevant checks. A1 will not assume that additional facial recognition or biometric verification is included within its particular TrustID service unless this has been confirmed.

A1 will ensure that verification results are recorded securely and that staff understand the distinction between identity verification and the statutory Right to Work checking requirements.

TrustID's privacy notice states that it may process images of identity documents, selfies, identity particulars and, for some services, biometric facial matching and AI-assisted verification. This describes optional capabilities across its services and does not establish that A1 uses every capability. TrustID has confirmed that A1's Digital Right to Work service excludes electronic address verification, PEP/sanctions screening and DBS checks.

If A1's chosen service uses biometric recognition to identify a person, A1 must document both an Article 6 lawful basis and an appropriate Article 9 special-category condition, and assess whether a data protection impact assessment (DPIA) is required. Obtain provider and processor documentation and assess any genuinely necessary alternative verification method.

5. Transparency and sharing

Candidates must receive a candidate privacy notice at or before collection. A1 will explain the purpose of checks, the information collected, lawful bases, relevant special-category conditions, recipients, international transfers, retention and rights. Material changes to data use must be explained before the changed processing starts.

A1 shares candidate information with prospective practices or corporate groups where necessary for introductions or legal compliance, taking account of confidentiality, minimisation and security. It may share information with TrustID, IT/cloud suppliers, professional advisers and relevant authorities where lawful. Sharing a candidate CV or verification material must follow a documented process and should avoid unnecessary passport copies.

6. Security and retention

Personal information is held in access-controlled recruitment and cloud systems. Staff use strong authentication, appropriate device security and secure transfer methods. Personal data must not be copied into personal accounts or shared over informal messaging without an approved security arrangement. A1 must maintain access permissions, deletion controls, staff awareness and supplier assurance.

A1 Locums will retain personal information only for as long as reasonably necessary for recruitment, placement administration, legal compliance and legitimate business purposes.

Candidate records will be reviewed periodically to ensure that information remains accurate, relevant and necessary. Active candidate records may be retained while individuals remain registered and available for suitable opportunities.

Inactive candidate records will normally be reviewed after 12 months of inactivity, with deletion or anonymisation considered after 24 months unless there is a documented reason for continued retention.

Right to Work verification records, placement information and financial records will be retained in accordance with applicable legal requirements and A1's approved Data Retention Schedule.

Where A1 is legally required to retain prescribed Right to Work evidence, it will retain that evidence for the relevant statutory period. Other identity verification material will be retained only for a justified period.

Records will be securely deleted or anonymised when no longer required

7. Individual rights, incidents and governance

A1 supports rights of access, correction, erasure, restriction, objection, portability and rights relating to automated decisions as applicable. Requests should be logged and normally answered within one month, subject to lawful extensions and exemptions. Staff must escalate requests to the designated privacy contact immediately.

Suspected personal data breaches must be reported internally without delay, investigated and documented. A1 must notify the ICO within 72 hours of awareness where notification is legally required and inform affected individuals where there is a high risk to their rights and freedoms.

This policy is reviewed at least annually and when services, suppliers or the law change. A1 maintains a processing register, privacy notices, supplier/processor agreements, retention schedule, breach log, and DPIAs where required.

8. Approval details

Policy Owner: Clare Alderton, Managing Director

Data Protection Contact: info@a1locums.com

Approval Date: 1st October 2026

Next Review: October 2027, or earlier if there are significant changes to legislation or A1's processing arrangements.

Related Documents: Candidate Privacy Notice, Data Retention Schedule, TrustID documentation and internal Right to Work procedure.

Appendix 1

A1 Locums will retain personal information only for as long as reasonably necessary for recruitment, business administration and legal compliance. Records will be reviewed and securely deleted or anonymised when no longer required. The following periods are proposed internal arrangements rather than universal statutory retention periods.

Record	Proposed retention
Active candidate records	While actively registered; review annually
Inactive candidate records	Review after 12 months; normally consider deletion after 24 months
RTW statutory evidence	Relevant engagement period plus two years, where the statutory rule applies
Other identity verification records	Defined, proportionate period based on the purpose of verification
Placement and booking records	Normally six years after the relevant transaction or engagement ends, subject to review
Financial/accounting records	Generally six years, subject to applicable statutory requirements
Unsuccessful registrations	Normally review and delete after six months unless continued retention is justified

The Managing Director, Clare Alderton, will oversee annual reviews of retained personal information and ensure that records are deleted or anonymised in accordance with this schedule.