KinMatch™

Security and data protection for agencies

KinMatch is built around safeguarding and to UK GDPR, for organisations that handle children's data. Every measure below is live today.

Independently certified

- Certified to the UK government-backed Cyber Essentials scheme (whole organisation, November 2026; certificate eb9d5359-eb99-483d-a286-6518cd77f2cf), so our baseline technical controls are assessed against a recognised standard, not just asserted.
- Registered with the Information Commissioner's Office (McTip IT Limited, ZB098611).

Accounts and access control

- Authentication through a specialist identity provider (Clerk), with multi-factor authentication available.
- Role-based permissions: Administrator, Manager, Supervising Social Worker, Child's Social Worker, Safeguarding Lead, Recruitment Officer, plus a view-only role. New users start view-only; only permitted roles can change records.
- Unlimited named staff logins, so every action is attributable to a person. No shared accounts.
- Deactivated users and suspended organisations are blocked at the server, not merely hidden in the interface.
- The platform operator console is kept separate from your organisation's workspace.

Your data stays yours

- Strict per-organisation isolation. You see only your own records, and referrals only where a local authority has shared them with you.
- Held in a dedicated UK (London) database, encrypted in transit and at rest, with automated backups.
- Your records are never sold or passed on. You can export your data at any time, at no cost.

Children's data is minimised

- Children are stored by initials and an anonymised reference only. A full name is never stored.
- Where the optional AI assistant reads a pasted referral, contact details and identifiers (email addresses, phone numbers, NHS or National Insurance numbers, case references) are removed before anything leaves our servers. AI assistance is controlled per organisation.
- The software ranks and explains options. A qualified person always makes the decision.

Tamper-evident audit trail

- Every action is recorded in an append-only log, sealed into a cryptographic hash chain, then independently timestamped by an external authority. Any change, deletion or reordering of a past record is detectable, even by us.
- Audit records export cleanly for Ofsted scrutiny and internal review.

Safe intake, safe attachments

- Inbound referral email is protected by a shared secret and fails closed if it is not configured.
- Password-protected or encrypted attachments are detected and flagged for a person to handle. Attachment contents are never stored, only safe metadata.

Protection against abuse

- Public forms are guarded by layered anti-spam measures (a hidden honeypot field, signed timing checks, content heuristics, optional Cloudflare Turnstile), together with rate limiting.

Verification

- Agencies are verified against the Ofsted register, Companies House and the Charity Commission.