Client Data Retention and Bina Chat

BP-CLIENT-RET-2026-11-07-v2 | Effective 7 November 2026 | Review 7 February 2027

Purpose

BP-PUB-09-20261106-v1 · Owner: Directors and responsible data contact

Download this policy as PDF

Purpose and access

Bina controls its recruitment, employment, bookings and learning records where it determines the purpose and means. We collect necessary information, give service-specific privacy notices and restrict access by role. The hirer normally controls its own care or education records. Ask admin@binapathways.co.uk or 07337 541218 about the rule applying to your data.

Retention rules

Unsuccessful applications: normally six months after decision. Optional talent pool: up to 12 months with informed participation. Ordinary employment, payroll, invoice and claims records: normally the justified six-year category period. Right-to-work copies: employment plus at least two years. Full DBS information: normally no longer than six months after the decision; a limited justified check log is separate. Raw attendance coordinates: normally 30 days after shift closure. Routine support chat: six months after closure. Security logs: normally 90 days.

Special categories and holds

Health, safeguarding, school allegation and litigation records follow their specific statutory duties, risk-based periods and legal holds. A hold identifies purpose, records, owner and review date; it is not indefinite permission to retain everything. The governance manual contains the full category schedule, including learning records and backup rotation.

Security and suppliers

Use individual authorised accounts, MFA where supported, secure devices, recipient checks and approved sharing routes. Record processors, locations, security, deletion and lawful transfer safeguards. Do not claim UK-only storage without evidence. Do not place bank, health, identity or care records in public enquiries or personal messaging.

Rights and breaches

Requests are normally answered within one month, subject to lawful conditions and extensions. Report a suspected breach immediately. Bina records awareness, risk, containment and whether ICO notification is required, normally within 72 hours where the legal threshold applies. Secure deletion is logged and checked; signed history and valid certificates are not silently rewritten.

Related controlled procedures: Governance manual sections 7 to 12; Staff and customer privacy notices. Controlled internal procedures can be requested from admin; personnel records are not published.

Chat records and the purposes of access

Bina records verified account identity, company and department details, conversation membership, messages and attachments, booking actions, delivery/read events, security events and investigation access records. These support work communication, staffing administration, service security, fair complaint handling and necessary safeguarding investigations. Client–staff, client–management and management–staff work conversations retain existing Bina management and department oversight. Access must be used for an authorised work purpose; a role or technical capability is not permission to browse out of curiosity. Staff-only conversations require the separate director-authorised control described above.

Lawful basis and proportionate investigation

Bina records the applicable lawful basis for each purpose. Routine staffing administration and proportionate security or complaint handling may rely on legitimate interests after a documented necessity and balancing assessment; legal obligation is used only where a specific duty applies. A client supply contract is not automatically a contract basis for processing a worker’s information. Before investigation access is enabled, the director must record the concern, why access is necessary, the selected conversation, investigators and duration, and consider a less intrusive route. Complete a DPIA where required and identify any Article 9 condition, Article 10 authority and associated UK-law requirements before processing the relevant sensitive information. Staff acknowledgement is not consent to surveillance and does not replace these assessments.

Limits on access and retained evidence

Investigation access exposes the selected conversation history and available attachments during the authorised period, including new messages while access remains active. The current control does not restrict access to selected dates within a conversation. The director must consider this scope before granting it. Switching access off ends further application access; it cannot withdraw a lawful copy or information already seen. Necessary retained evidence must be placed in the restricted case record, limited to the purpose and reviewed under the applicable retention schedule. No personal app, private device content or unrelated conversation is included. Do not use this control for covert monitoring.

Acknowledgement and optional choices

Staff acknowledge receipt and understanding of the current handbook and chat policy. Clients acknowledge the operational and privacy information, and an authorised company administrator separately accepts revised contractual terms where required. Nobody may accept or sign for another user. Earlier signed versions and receipts remain historical evidence. Optional marketing, device notification permission and any genuinely optional consent remain separate, may be declined without preventing ordinary account access, and can be changed through the relevant control. Essential service and policy notices are operational communications rather than marketing.

Retention and privacy rights

Chat participants cannot delete sent messages, attachments or conversations through the app. Own-message text editing ends two minutes after original sending; edits retain their audit history. This user-interface restriction does not remove data protection rights or authorise indefinite retention. Routine closed support conversations follow the published review schedule; operational chat and necessary investigation evidence follow their applicable justified category, with a specific legal hold where required. Contact admin@binapathways.co.uk for access, correction, objection, restriction, deletion or other applicable rights. Bina will assess the legal conditions and any necessary protection of another person’s information and explain any limitation. You may complain to the ICO.

Client work chat boundaries

Clients and eligible staff may communicate for staffing and assignment purposes. Bina management and departments retain oversight of client–staff and client–management work conversations for authorised operational, service, security and safeguarding purposes. Clients cannot see another company’s conversations or staff-only conversations. Staff-only investigation controls apply solely to staff-to-staff conversations and do not switch off oversight of client work conversations. Bina must use access proportionately and follow the privacy notice, confidentiality obligations and applicable law.