

## Privacy Policy 2024

### Contact Details

This privacy policy deals with the collection and use of Personal Identifiable Information (PII) by Bancroft Ltd, 32 Harbour Exchange Square, Harbour Island, London. E14 9GE under the General Data Protection Regulations (GDPR) 2018. Bancroft Ltd have been identified as the Data Controller of PII collected and processed and Mr. Brett Cockrell has been appointed as the companies representative responsible. The company has appointed Mr. Jason Dodd to undertake this role of Data Protection Officer (DPO) to be the point of contact for the Supervisory Authority and provide advice, training and awareness of the regulations to the company and its employees.

### Whose PII Data is Collected

The categories of individuals which PII is held are:

Employees, Directors, Apprentices, Work Experience Students, Recruitment, Business Contacts, Contractors, Agency Labour and Emergency Contacts.

The Purpose, Type and Legal Basis which we use PII is detailed below:

Purpose	Type of PII that may be processed	Legal Basis
Recruitment	Information concerning your application and/or CV and our assessment of it, your references, any checks we may make to verify information provided or background checks and any information connected with your right to work in the UK. If relevant, we may also process information concerning your health, any disability and in connection with any adjustments to working arrangements. Post-employment reference as requested from yourself or agency working on your behalf.	Legal Obligation Legitimate Interests
Your employment contract including entering, performing and changing it	Information on your terms of employment including your pay and benefits, such as your participation in pension arrangements, medical insurance and any bonus or share schemes	Contract Legal Obligation Legitimate Interests
Contacting you or others on your behalf	Your address and phone number, emergency contact information and information on your next of kin. Employment status and dates for personal information matters such as mortgages, loans etc. authorised by yourself	Contract Legitimate Interest
Payroll administration and other financial benefits	Information on your bank account, pension contributions and on tax and national insurance. Payroll documents such as Pay slips, P60, P11d and P45 forms which shall be directly emailed to your personal email address provided to us. Information on attendance, holiday and other leave and sickness absence.	Contract Legal Obligation Legitimate Interests



Supporting and managing your work, performance and any health concerns during and after your employment	<p>Information connected with your work, anything you do at work and your performance including records of documents and emails created by or relating to you and information on your use of our systems including computers, laptops or other devices.</p> <p>Management of information regarding you including notes of meetings and appraisals records.</p> <p>Information relating to your compliance with our policies.</p> <p>Information concerning disciplinary allegations, investigations and processes and relating to grievances in which you are or may be directly or indirectly involved.</p> <p>Information concerning your health, including self-certification forms, fit notes and medical and occupational health reports.</p>	<p>Consent</p> <p>Contract</p> <p>Legal Obligation</p> <p>Legitimate Interests</p>
Physical and System Security	<p>CCTV images, Records of key fob entry system, Time &amp; Attendance Software including Photograph, Signature (Optional) and an Encrypted Template of a fingerprint.</p> <p>Records of use of our systems including computers, phones and other devices and passwords.</p>	<p>Legal Obligation</p> <p>Legitimate Interests</p>
Monitoring of diversity and equal opportunities	<p>Information on your nationality, racial and ethnic origin, gender, sexual orientation, religion, disability and age.</p>	<p>Legitimate Interests</p>
Monitoring and investigating compliance with policies and rules – both generally and specifically	<p>We expect our employees to comply with our policies and rules and may monitor our systems to check compliance. We may also have specific concerns about compliance and check system and other data to look into those concerns (e.g. log in records, records of usage, emails, documents and CCTV images).</p>	<p>Legitimate Interests</p>
Disputes and legal proceedings	<p>Any information relevant or potentially relevant to a dispute or legal proceeding affecting us.</p>	<p>Legal Obligation</p> <p>Legitimate Interests</p>
Day to day business operations including marketing and client relations	<p>Information relating to the work you do for us, your role and contact details including relations with current or potential clients. This may include a photograph of you for internal or external use.</p>	<p>Legitimate Interests</p>
IT technical support, back up and disaster recovery	<p>Any information required to resolve the technical difficulty experienced</p>	<p>Legitimate Interests</p>
Maintaining Business Contacts with Clients, Suppliers and Contractors	<p>Information relevant to keeping good business relationships which include your name, job title, contact details and address</p>	<p>Legitimate Interests</p>
Accident or Incident Information resulting in injury to a Sub-Contractors personnel	<p>Medical evidence of injury sustained, photographs, witness statements, contact details, qualifications and training records</p>	<p>Legal Obligation</p> <p>Legitimate Interests</p>

### **Who we share PII with**

Employees, Directors, Consultants, Apprentices and Work Experience Students, PII shall be shared with HMRC for Tax Compliance, NatWest Bank and your Bank/Building Society for Automated Clearing System (Bacs), Pension information for Auto Enrolment with the appointed scheme, Standard Life for Bancroft Pension, Healthcare provider (non-medical data), Child Maintenance Services or CSA and any relevant court orders where applicable. We shall also share your PII as a 3<sup>rd</sup> party reference, where you have identified the company as a reference. We shall only provide the PII after consultation with you. If you are required to attend a Medical Practitioner by the company, we shall provide the necessary PII for your appointment. Any training requirements identified, the necessary PII shall be provided to any external training provider for the course. Business Contacts, Contractors and Emergency Contact PII shall not be shared with any other companies. Recruitment Candidates PII may be shared with the Recruitment Agency which you have been registered with (where applicable). Agency Labour PII shall be shared with the approved Labour Agency only.

### **Transfers of PII**

Transfers of your PII are to our Cloud Storage Providers of our backup systems, which includes; DATTO for OneDrive and Emails back-ups stored within the UK, Coredata for Server back-ups stored within the UK. Microsoft 365 hold our live data including live emails and this is stored within UK data centers.

### **Retention Times**

The retention period for holding PII is detailed within our Retention Policy with all PII held for no longer than 15 years.

### **Technical & Organisational Security Measures**

The Company has implemented appropriate internal security procedures restricting access to and disclosure of PII. The sever files are managed by a User Access Management Software system for restricting access which includes Active Directory, Password Protected, Smart-card and Multi Factor Authorisation. Physical controls include 24-hour security on reception, security key fob access, key code access to each floor, digital key code to our server room and CCTV monitoring. All filing cabinets are key lockable within each department. All off-site Back-ups are held within the secure location by our Cloud Storage Providers and are encrypted at rest. The off-site storage location has 24-hour security protection and appropriate other security restrictions to prevent access.

### **Your Rights**

GDPR provides individuals whose PII is held by the Company specific rights to access and rectify any PII held about them. These include: The right to be informed, access, rectification, erasure, restrict processing, data portability, object or rights in relation to automated decision making and profiling. Under GDPR every individual has the right to lodge a complaint with the Supervisory Authority within their habitual residence, place of work or of an alleged infringement of GDPR. Within the UK this is the Information Commissioner's Office.

If you have any questions about this privacy policy, you can email us at [office@bancroft.uk.com](mailto:office@bancroft.uk.com) or call 020 87092500 to contact the company DPO.

The company will review and revise the policy as and when necessary, or at regular intervals of no longer than 12 months.

Signed:

Name: Barry Martin

Title: Managing Director

Date: 11<sup>th</sup> January 2024