

Privacy Notice

Date:	10 th January 2025
Review date:	10 th January 2026
Approved by:	Rob Grays – Chief Executive Officer

Contents

Purpose.....	2
Definitions	2
Data Protection Principles	2
Information Collected.....	2
Collection of Personal Information.....	3
Information Use.....	4
Sensitive Personal Information	5
Convictions	5
Automated Decision-Making.....	6
Data Security	6
Data Retention	7
Rights of Access, Correction, Erasure and Restriction.....	8
Rights to Withdraw Consent	9
Data Protection Officer	9
Duty to Inform Us of Changes	9

Purpose

Banquo Ltd (Part of Prospero Group Limited) (Company Number 13150451) of 3rd Floor, 15 Worship Street, London, England, EC2A 2DT is a “Data Controller”. This means that we are responsible for deciding how we hold and use personal information. This privacy notice outlines how and why your personal data will be used, under the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**).

Definitions

Care and Support Services – taken to mean recruitment activity provided by Banquo Ltd on behalf of Clients and Employees including, but not limited to, advertising of roles, vacancy matching and provision of work-related training.

Contact – an individual employed by a Client.

Client – an organisation with the potential to engage with Banquo Ltd to purchase Care and Support Services. This includes, but is not limited to, Local Authorities, Care Homes, Parents/Carers and Private Sector organisations.

Employee – an individual receiving work, delivered by Banquo Ltd. This includes, amongst others: Care Assistants, Support Workers and Registered Managers.

Data Protection Principles

We will comply with data protection law and principles, which means that your data will be:

- a) Used lawfully, fairly and in a transparent way
- b) Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- c) Relevant to the purposes we have told you about and limited only to those purposes
- d) Accurate and kept up to date
- e) Kept only as long as necessary for the purposes we have told you about
- f) Kept securely

Information Collected

Personal data means any information about an individual from which that person can be identified.

Contacts

In connection with providing Care and Support Services to our Clients, we will collect, store, use, and transfer the following categories of personal information about you:

- **Identity Data** includes name and title
- **Contact Data** includes address, email address and telephone number
- **Profile Data** includes details of your interests, preferences, and feedback
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

Employees

In connection with your application for work, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae, registration form and/or covering letter
- **Application Data** (information you have provided on our application form) includes name, previous surnames, title, address, telephone number, personal email address, date of birth, gender, and photographs.
- **Recruitment Data** (information you have provided on our application form) includes employment history (job titles, work history, training records, and professional memberships), qualifications, references, national insurance number, right to work information and documents, DBS results, overseas police check, contact name and telephone number for emergency contact, any details relating to disqualification from working with children subject to the relevant legislation, medical information relating to capability to carry out the role, and professional registration details.
- **Interview Data** includes any information you provide to us during an interview.
- **Payroll Data** includes booking information including payroll company, name, payroll number, rate of pay, associated charge rate, contact details, booking email confirmation, time sheets.
- **Communication Data includes** any communications between you and Banquo Ltd.
- **Marketing Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your race or ethnicity (where included on ID).
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.
- Information provided as part of the safeguarding or allegations management process.
- Information about Trade Union membership.

We do not envisage processing any data relating to your religious beliefs, sexual orientation and political opinions. However, in the event that we become a controller of any such data, it will be handled in accordance with the UK GDPR.

Please note that you can amend/update any of your information we hold by contacting our Data Protection Officer.

Collection of Personal Information

Contacts

We collect personal information about Contacts from the following sources:

- You, the Contact
- Client website
- Other public facing websites
- Any communications between you and Banquo Ltd

Employees

We collect personal information about Employees from the following sources:

- You, the Employee.
- uCheck Limited (our background check provider), from which we collect the following categories of data: all information contained within background checks they are instructed to carry out.
- Disclosure and Barring Service in respect of criminal convictions.

- Your named referees, from whom we collect the following categories of data: performance related information, general conduct information e.g. punctuality and attendance records. Please note that you can request a copy of our reference request form prior to it being sent to your named referee.
- Open Source Data from a publicly accessible source, including but not limited to: job boards, social media sites such as Facebook, LinkedIn, Twitter, Instagram, YouTube and Spotify, personal recommendations and face-to-face contact at recruitment events.
- Any communications between you and Banquo Ltd

Information Use

Contacts

We will use the personal information we collect about you:

Purpose/Use	Type of data	Legal basis
As part of the Care and Support Services process	<ul style="list-style-type: none"> • Identity Data • Contact Data • Profile Data 	<ul style="list-style-type: none"> • Necessary for our legitimate interests (to perform the Care and Support Services)
For timesheet and invoicing activities	<ul style="list-style-type: none"> • Identity Data • Contact Data 	<ul style="list-style-type: none"> • Necessary for our legitimate interests (to recover debts due to us)
For relevant Client sector marketing activity (with your consent)	<ul style="list-style-type: none"> • Identity Data • Contact Data • Marketing and Communications Data 	<ul style="list-style-type: none"> • Legitimate interest (to provide similar job related content to Contacts)

Employees

We will use the personal information we collect about you:

Purpose/Use	Type of data	Legal basis
As part of the Care and Support Services process	<ul style="list-style-type: none"> • Application Data • Recruitment Data • Interview Data • Communication Data • Payroll Data 	<ul style="list-style-type: none"> • Necessary for performance of a contract (the Care and Support Services)
Checking Right to Work in the UK	<ul style="list-style-type: none"> • Application Data • Recruitment Data 	<ul style="list-style-type: none"> • To comply with a legal obligation (preventing illegal working)
Verifying DBS status Background checks Regulatory checks	<ul style="list-style-type: none"> • Application Data • Recruitment Data • Open Source Data 	<ul style="list-style-type: none"> • To comply with a legal obligation (to ensure you can work as a teacher; work with children; or are not otherwise prevented from working in certain environments by law)

For relevant marketing activity (with your consent)	<ul style="list-style-type: none"> • Application Data • Communication Data • Marketing Data 	<ul style="list-style-type: none"> • For prospective candidates: Consent must be obtained. • For existing candidates: legitimate interests and soft opt-in under the Privacy and Electronic Communications Regulations 2003 (PECR).
---	--	---

Having received your CV, covering letter and your application form (where applicable), we will then process that information to decide whether you meet the basic requirements to be shortlisted for our Care and Support Services. If you do, we will decide whether your application is strong enough to invite you for an interview (where applicable). If we decide to call you for an interview, we will use the information you provide to us at the interview to decide whether to provide you with Care and Support Services. If we decide to offer you Care and Support Services, we will then take up references, carry out a criminal record check and any other check (where applicable) before confirming you have been accepted as a Employee for our Care and Support Services.

Sensitive Personal Information

Employees

We will use your particularly sensitive personal information in the following ways:

- We will use information about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during an interview.
- We will use information about your national or ethnic origin to ensure you have the relevant right to work within the location of the role.
- We will use information regarding any medical condition you declare to us in order to assess your capability to carry out the role/s for which you wish to be considered.
- We will use the results provided from your DBS check to assess your suitability for the role/s for which you wish to be considered.

Convictions

Employees

We envisage that we will process information about criminal convictions.

We will collect information about your criminal convictions history if we would like to offer you a role conditional on checks and any other conditions, such as references, being satisfactory. We are required to carry out a criminal records check in order to satisfy ourselves that there is nothing in your criminal convictions history which makes you unsuitable for the role. In particular:

- a) We are legally required to carry out criminal record checks for those carrying out a role which would involve them working with vulnerable people. Please note that you will be notified in advance of us applying for such check
- b) The roles of healthcare professionals are ones which are listed on the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (SI 1975/1023) and are also specified in the Police Act 1997 (Criminal Records) Regulations (SI 2002/233) so are eligible for a standard or enhanced check from the Disclosure and Barring Service

When processing such data appropriate safeguards will be maintained in accordance with the UK GDPR requirements.

Automated Decision-Making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data Sharing

Contacts

We will only share your personal information with the following third parties for the purposes of the Care and Support Services process, where it is necessary to administer the working relationship with you, where it is a legal obligation, or where we have another legitimate interest in doing so:

- Our IT provider
- Our CRM provider
- Membership / Trade Associations
- Auditors / Inspectors appointed by the Client, Trade Association or Government Body
- Employees
- Third parties to whom we may choose to sell, transfer or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy policy.

Employees

We will only share your personal information with the following third parties for the purposes of the Care and Support Services process, where it is necessary to administer the working relationship with you, by law, or where we have another legitimate interest in doing so:

- Our IT provider
- Our CRM provider
- Membership / Trade Associations
- Auditors / Inspectors appointed by the Client, Trade Association or Government Body
- Clients
- Payroll provider
- Any third-party service provider required as part of our Safer Recruitment process – for example: to process your enhanced DBS application.

Whenever we transfer your personal data out of the UK to countries which have laws that do not provide the same level of data protection as the UK law, we always ensure that a similar degree of protection is afforded to it by ensuring that safeguards are implemented.

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal

information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality. Details of these measures may be obtained from our Data Protection Officer.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data Retention

We retain your personal information so that in the event of a legal claim, we have evidence that we have not discriminated against you on prohibited grounds and that we have conducted the Care and Support Services exercise in a fair and transparent way.

After the retention period has lapsed, we will securely destroy your personal information in accordance with our Data Retention Policy.

	Data Type	Data definition or examples	Processing Purpose	Standard Retention Period
Employee	Personal data	<p><i>Includes but not limited to:</i></p> <p>Application Data - direct application, job board applications and downloads from CV Databases.</p> <p>Recruitment Data; Interview Data - registration form, interview notes, CV, photo, signed Rules of Engagement and Code of Conduct, emergency contact details and referee details.</p> <p>Application Data; Recruitment Data - passports, visa, NI number proof, birth certificate, sponsorship details, biometric residence permit, driver's licence, proof of address, proof of name change, qualifications and training certificates.</p> <p>Communication Data.</p>	Performance of a contract.	Two years from last day of work.
	Special category personal data	<p><i>Includes:</i></p> <p>Professional body membership, medical data including any reasonable adjustments, GP letter, risk assessments, enhanced DBS check and rehabilitation of offenders and Childcare Disqualification declaration.</p>	<p>Legitimate interests.</p> <p>Legal obligation - Safeguarding and Child Protection.</p>	<p>Two years from last day of work.</p> <p>Where relevant to safeguarding and child protection, indefinite extension on a case-by-case basis.</p>

	Safeguarding	<p><i>Includes but not limited to:</i></p> <p>Online search information (as required under KCSIE 2022), prohibition checks, professional conduct & safeguarding concerns, responses from referees, feedback from Clients and any other third party (for example – Local Authority Designated Officer or police).</p>	Legal obligation - Safeguarding and Child Protection.	Until normal retirement age or 10 years, whichever is the longer, with indefinite extension on a case-by-case basis (NSPCC Child protection records retention and storage guidelines 2023).
	Payroll and invoicing	<p><i>Includes:</i></p> <p>Booking information including payroll company, name, payroll number, rate of pay, associated charge rate, contact details, booking email confirmation, Copies of time sheets, both electronic submission and paper versions. May include Employee's name, pay details, hours worked and contact details.</p>	Performance of a contract. Legal obligation - HMRC.	Seven full tax years from last day of work.
Contacts	Personal data	<p><i>Includes but not limited to:</i></p> <p>Name, contact information including telephone number, email addresses and postal address, job title, employer, audio recordings of telephone conversations, preferences and interests, and any other information provided by the Client.</p>	Legitimate Interests.	Duration of contract whilst data directly relevant to provision.
	Safeguarding (where Contact raises a concern about an Employee)	<p><i>Includes but not limited to:</i></p> <p>Name, contact information including telephone number, email addresses and postal address, job title, employer, audio recordings of telephone conversations, and any other information provided by the Client relating to the safeguarding concern.</p>	Legal obligation – Safeguarding and Child Protection	Where relevant to safeguarding and child protection, indefinite extension on a case-by-case basis.
	Payroll and invoicing	<p><i>Includes but not limited to:</i></p> <p>Name, contact information including telephone number, email addresses and postal address, job title, employer,</p>	Legal obligation - HMRC.	Seven full tax years from last day of work.

Rights of Access, Correction, Erasure and Restriction

Your rights in connection with personal information.

Under certain circumstances, by law you have the right to:

- a) **Request access** to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it
- b) **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected
- c) **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below)
- d) **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes
- e) **Request the restriction** of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it
- f) **Request the transfer** of your personal information to another party

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer in writing at dataprotectionofficer@banquoltd.com.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

Rights to Withdraw Consent

Where you provide us with consent in relation to us processing your personal information for the purposes of recruitment or for providing marketing materials, you have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact the DPO on dataprotectionofficer@banquoltd.com.

Once we have received notification that you have withdrawn your consent, we will no longer process your personal data (including, where you are an Employee, your application) and, subject to our retention policy, we will dispose of your personal data securely.

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact the DPO on dataprotectionofficer@banquoltd.com.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Duty to Inform Us of Changes

We keep our privacy policy under regular review. It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new address or email address.