

Recruitment Privacy Notice

Christie & Co take your privacy seriously. This Privacy Policy covers our treatment of personally identifiable information (personal data) that we collect during the recruitment process at Christie & Co.

Christie & Co is the controller of your personal data for recruitment activities.

This notice applies only to recruitment activities carried out by Christie & Co and does not cover other group entities, which maintain their own privacy notices.

Registered address:

White Friars House, 6 Carmelite St, Temple, London, EC4Y 0BS

Data Protection Officer:

Nigel Astbury

Email: dpo@christie.com

What this Privacy Policy covers

This notice explains how we process personal data relating to job applicants, including candidates applying directly or through third parties.

We are committed to ensuring that the data we collect is appropriate and used only for recruitment purposes.

What Personal Data We Collect

We may collect and process the following personal data:

- Name, address, email address, and telephone number
- CV, employment history, qualifications, and skills
- Current and desired salary
- Information from publicly available sources (e.g. LinkedIn profiles)
- Records of communications during the recruitment process
- Application forms, cover letters, and correspondence
- Interview notes and assessment outcomes (including tests or task submissions)
- Right to work, visa, and immigration status documentation
- References and background check information (where required)
- Recruitment system records (e.g. application status, communications)
- Diversity and equal opportunities information (where voluntarily provided)

For applicants to Valuation Services roles, we will process personal data to conduct credit, bankruptcy, and Disclosure and Barring Service (DBS) checks as part of our recruitment process. This processing is carried out to assess suitability for the role and meet our legal and regulatory obligations.

How We Collect Your Data

We collect personal data from:

- You directly (applications, CVs, interviews)
- Recruitment agencies or job boards
- Referees
- Publicly available sources (e.g. LinkedIn)
- Internal referrals

How We Use Your Data (Legal Basis)

We only process your personal data where we have a lawful basis under UK GDPR.

We process your personal data for recruitment purposes under the following lawful bases:

- ❖ **Legitimate interests** – to assess your suitability for employment
- ❖ **Contractual necessity** – to take steps prior to entering an employment contract
- ❖ **Legal obligations** – to verify your right to work and comply with employment laws
- ❖ **Consent** – where required (e.g. for keeping your details on file for future roles)

Special category data (e.g. diversity data) is processed only where permitted by law and with your explicit consent, typically for equal opportunities monitoring. Diversity monitoring data is handled confidentially and, where possible, anonymised.

Where we rely on legitimate interests, we ensure these are balanced against your rights.

How Your Data Is Stored

Your personal data is securely stored and managed within our HR system, Cezanne HR, which is used to administer recruitment processes.

We apply appropriate technical and organisational measures to protect your data, including:

- Access controls
- Secure systems and hosting
- Encryption where appropriate
- Staff training

These measures align with our wider approach to data security.

Information Sharing and Disclosure

We do not sell or rent your personal data.

We may share your data with:

- Internal hiring managers and HR teams
- Recruitment agencies involved in your application
- Background screening providers (if applicable)
- IT system providers, including Cezanne HR
- Professional advisers (e.g. legal or audit)
- Regulators or law enforcement where required

All third parties are required to process personal data in accordance with applicable data protection laws.

International Transfers

Where personal data is transferred outside the UK or EEA, we ensure appropriate safeguards are in place, such as:

- Adequacy decisions
- UK International Data Transfer Agreement (IDTA)
- Standard Contractual Clauses

We also carry out transfer risk assessments and apply additional safeguards where necessary.

Data Retention

We retain personal data only for as long as necessary.

Unsuccessful candidates: typically, up to 12 months after the recruitment process.

Successful candidates: data will be transferred to employee records and retained in line with our employee retention policy.

Former employees: personal data is retained for 6 years following the end of employment, after which it is securely deleted.

Longer retention may apply where required by law.

Automated Decision-Making

We do not carry out automated decision-making or profiling in recruitment that produces legal or similarly significant effects.

Your Data Protection Rights

You have the right to:

- Access your personal data
- Rectify inaccurate data
- Request erasure
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent at any time

You can exercise your rights by contacting:

dpo@christie.com

There is no charge for exercising your rights.

Complaints

You have the right to lodge a complaint with:

Information Commissioner's Office (ICO)

www.ico.org.uk

Changes to This Notice

We may update this Recruitment Privacy Notice from time to time. Any updates will be published accordingly.