Thomas Gray Limited
Privacy Notice (Internal)

Introduction

We are Thomas Gray Limited (Registered in England & Wales No. 07839720) of Crest House, 53 Station Road, Egham, Surrey, TW20 9LG.

This Privacy Notice sets out the basis on which we use personal data in respect of our internal recruitment and employment procedures.

We reserve the right to update this Privacy Notice from time to time. Where appropriate, we shall contact you to notify you of any material changes to the Privacy Notice. You should check for updates periodically to ensure that you understand (i) how we are using your personal data and (ii) your legal rights around our usage of such personal data.

Who Should Read This Privacy Notice?

You should read this Privacy Notice if you are:

- **An Applicant** for employment
- **An Employee,** including any onsite temporary worker, casual staff, consultant, apprentice etc.

If you are a Candidate, Client Contact or Supplier Representative, you should refer to our external Privacy Notice instead. This is available to view on our website at www.tglsearch.com/policies.

Definitions

This Privacy Notice uses the following defined terms:

Applicant means a person who has submitted an application or enquiry, directly or indirectly, with a view to becoming an Employee.

Data Protection Legislation means (i) the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in the UK and then (ii) any successor legislation to the GDPR or the Data Protection Act 1998.

Employee means a current or former employee of ours, including permanent, fixed- term, temporary and casual staff who are or have been (i) employed or otherwise engaged by us or (ii) supplied to us by a third- party employment business to work within our offices. We use the term "Employee" within this Privacy Notice to refer generally to someone who works for us or provides services to our business personally but nothing in this Privacy Notice is intended to affect your employment status in any respect.

Third-Party Services Provider means any relevant third-party business which provides services to us, including our:

- Professional advisers including accountants, tax advisors and lawyers;
- Pension provider;
- Provider of employee benefits;
- Insurers;
- IT services providers and software providers;
- Independent consultants and subcontractors

How We Obtain Personal Data

If you are an **Applicant**, we may obtain personal data relating to you:

- Directly if you have:
  - Applied for an internal vacancy through our website; ○ Completed an application for employment form;
  - Sent your CV directly to us;
  - Attended an interview or assessment day with us.

- Indirectly from:
  - Third-party recruitment businesses;
  - Job boards and CV search databases, such as CV Library, Not Going To Uni, Total Jobs etc. ○ Professional networking sites, such as LinkedIn;
  - Third-party referees; and
  - Individuals who have recommended you to us.

If you are an **Employee**, we may obtain personal data relating to you:

- Directly from you in the ordinary course of your employment relationship with us

- Indirectly from:
  - Other employees within our business, such as your line manager, your colleagues and our senior managers;
  - Third Party Services Providers who process your personal data on our behalf; ○ Medical and occupational health practitioners and advisors;
  - Governmental bodies, such as HMRC, the Department for Work and Pensions and HMCTS; and
  - Background checking services such as the Disclosure and Barring Service.

Types of Information We Hold

If you are an **Employee** or **Applicant**, we may collect, store and process the following types of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and email addresses;
- Your gender, date of birth, marital status and nationality;
- Proof of your right to work in the United Kingdom such as copies of your passport and, where applicable, visa, residence permit or similar government documents;
- Proof of your identity and address;
- Your qualifications and certifications;
- Any information within your CV, cover letter and application form;
- Any other information captured during the recruitment process; and
- Academic, professional and personal references from third parties.

If you are an **Employee**, we may also collect, store and process the following types of personal information about you:

- Next of kin and emergency contact information;
- National Insurance number;
- Dates of employment or engagement;
- Details of the days and times which you have worked;
- Bank account details, payroll records and tax status information;
- Salary, annual leave, pension and benefits information;
- Location of employment or workplace;
- Employment records (including job titles, work history, working hours, training records and professional memberships);
- Remuneration and payment history;
- Performance information;
- Disciplinary and grievance information;
- CCTV footage and other information obtained through electronic means such as door access records;
- Geolocation data from any “connected” device or equipment belonging to us which you may use in the course of your employment or engagement with us;
- Information about your use of our information and communications systems; and
- Photographs.

If you are an Applicant or Employee, we may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions;
- Trade union membership;
- Information about your health, including any medical condition, disability, health and sickness records; and
- Information about criminal convictions and offences.

How We Use Personal Data

If you are an **Applicant** or an **Employee**, we may use your personal data to:

- Make a decision about your appointment or engagement;
- Determine the basis on which you may be employed or engaged by us, where applicable;
- Check that you are legally entitled to work in the United Kingdom;
- Verify the information which you have provided during the recruitment process;
- Carry out data analysis into Applicant attraction and conversion; and
- Carry out Equal Opportunities monitoring

If you are an **Employee**, we may also use your personal data to:

- Pay you and, where applicable, deduct tax and National Insurance contributions;
- Where applicable, provide benefits to you such as gym memberships, private healthcare etc;
- Liaise with your pension provider;
- Administer the contract we have entered into with you;
- Conduct business management and planning, including accounting and auditing;
- Conducting performance reviews, managing performance and determining performance requirements;
- Make decisions about salary reviews and compensation;
- Assess your qualifications for a particular job or task, including decisions about promotions;
- Gather evidence for possible grievance or disciplinary hearings;
- Make decisions about your future or continued employment or engagement;
- Make arrangements for the termination of our working relationship;
- Assess the need for and provide education, training and personal development;
- Deal with legal disputes involving you, or other employees, workers and contractors, including accidents at work;
- Ascertain your fitness to work;
- Manage sickness absence;
- Comply with health and safety obligations;
- Prevent fraud;
- Monitor your use of our information and communication systems to ensure compliance with our IT policies;
- Ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution; and
- Conduct data analytics studies to review and better understand employee retention and attrition rates.

If you are an **Employee**, we may also use your sensitive personal data in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws;
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits; and
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Thomas Gray Limited
Privacy Notice (Internal)

Our Lawful Basis for Processing Data

We are legally entitled to process your personal data where it is necessary for the performance of the contract for services or contract of service to which you are a party, either directly with us or, in some circumstances, with a third party such as an employment business. This includes any processing which may be necessary at the preliminary stage prior to you entering into a contract, provided that this is done at your request e.g. by submitting an application.

We may also process your personal data where it is necessary for compliance with a legal obligation to which we are subject, such as the obligation to maintain suitable business and financial records.

In accordance with Article 9 (2)(b) of the GDPR, we are entitled to process your sensitive personal data where we need to carry out our obligations or exercise our rights in the field of employment. Under very limited circumstances, we may also ask for consent to process your sensitive personal data.

Where We Process Personal Data

Your personal data is held and processed by us in the United Kingdom.

We have put in place appropriate safeguards to ensure that your data is only transferred to jurisdictions with enforceable data subject rights and effective legal remedies in respect of data privacy breaches. We will therefore only transfer your personal data to jurisdictions outside of the EEA where:

- There are binding corporate rules in place regarding the transfer of such data within the Group, in accordance with Article 47 of the GDPR. *This means that the data transfer is between group companies and those group companies have agreed to share that data in accordance with the rules specified by the European Commission.*

- The European Commission has made an adequacy decision in respect of such jurisdiction. *This means that the European Commission has pre-approved the data privacy regime in the relevant non-EEA country. At present, the European Commission-approved jurisdictions are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework).*

- The transfer of data is subject to the model contractual clauses adopted by the European Commission. This means that we have a data-sharing agreement in place which complies with the requirements set out by the European Commission; or

- You have expressly given informed consent to the transfer of such data. *This means that you have not only agreed to the transfer but have done so in the knowledge that your data may be transferred to a jurisdiction which does not give you the same degree of protection as you have within the EEA.*

Parties with Whom We May Share Data

We may share your personal data for legitimate purposes with:

- Our directors, officers and employees where it is appropriate and necessary to do so;
- Where applicable, any third-party company through which you are contracting;
- Third-Party Services Providers;
- Any third-party who you have engaged and to whom you have confirmed that we may provide personal data, such as your bank or mortgage advisor;
- Our clients, where it is reasonable and necessary to do so e.g. where we provide your business contact information or, in the event of a dispute, provide internal communications or explanations as to the actions which you have taken;
- Any third party to which we may be planning to transfer or sell a relevant part of our business;
- Governmental departments and agencies where we are permitted or required by law to do so.

If we share your information with any third party, we will require them to respect your data privacy and only use your data for the purpose for which it was provided or otherwise as permitted by law.

Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. All decisions which are made in the course of our business processes involve human intervention. We do not expect to make any decisions about you using automated means but will let you know if this changes.

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 the Data Protection Manager.

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 will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

If you are an **Applicant**, we will usually retain your personal data for three years from the date on which the recruitment decision is made, unless you become an **Employee**, in which case the provisions below shall apply.

If you are an **Employee** , our standard data retention period is three years from the date on which our working relationship ends. After this time, we will usually delete any personal data from our records which is no longer required. Where we are required to keep any information (i) for auditing or compliance purposes (ii) to comply with our contractual obligations to third parties or (iii) in respect of any potential or actual legal proceedings, we shall keep your data for as long as is strictly necessary for these purposes, which is typically for seven years from the date on which our working relationship ends.

In some circumstances we may completely anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

Rights of access, correction, erasure, and restriction

Your duty to inform us of changes. It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information. Under certain circumstances, you have the right to:

- Request **access** to your personal information (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. You will not usually have to pay a fee to access your personal information but we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

- 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.

- Request **erasure** of your personal information. This enables you to ask us to delete or remove personal information where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed or you have objected to the processing and there is no overriding legitimate interest for continuing the processing.

- **Object** to processing of your personal information where we are relying on a legitimate interest and you object on "grounds relating to your particular situation."

- Request the **restriction** of processing of your personal information. This enables you to ask us to block or suppress the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it or if you have also objected to the processing as above.

- Request the **transfer** of your personal information to another party when the processing is based on consent and carried out by automated means. This right is not usually applicable to any data processing carried out by TGL.

If you want to exercise any of the above rights, please contact the Data Protection Manager in writing. We will consider your request and confirm the actions which we have taken in response to such request.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is an appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Manager. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law. We will confirm the actions which we have taken in respect of any such request.

If you are unhappy with any aspect of the manner in which we have processed your personal data or dealt with your decision to exercise any of the rights set out in this section, you have the right to complain to the Information Commissioners Office in the United Kingdom. Their details are:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate) or, if you prefer to use a national rate number, 01625 545 745
Email: casework@ico.org.uk

Contacting Us

If you have any questions about this Privacy Notice, you can write to the Data Protection Manager, Matt Revett or Data Controller, Dani Mémé at Thomas Gray Limited, Crest House, 53 Station Road, Egham Surrey, TW20 9LG. Alternatively, you may telephone us on 01784 697 711 or email us at dataprotection@tglsearch.com.