

Privacy Notice for General Recruitment

What is the purpose of this document?

Howes Percival LLP (“the Firm” or “we”) is a “data controller”. This means that we are responsible for deciding how we hold and use personal data about you. You are being sent a copy of this privacy notice because you are applying for work with us (whether as an employee, worker, partner/member or consultant). It makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under UK data protection laws, including the Data Protection Act 2018.

Data protection principles

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

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

The kind of information we hold about you

Personal data means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

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

- The information you or a recruitment agent have provided to us in your curriculum vitae and covering letter (if applicable).

- Any information you may have provided on any application form or other document for recruitment purposes, including name, title, address, telephone number, and personal email address, date of birth, gender, employment history, qualifications, and referee details.
- Any information you provide to us during any interview or assessments/tests and any notes taken by interviewers (including scores or opinions regarding your suitability (if applicable)).
- If you attend an interview or are successful in your application, CCTV footage (at our Northampton and/or Norwich and/or Leicester offices) and details from our visitor signing in books at our premises.

We may also collect, store and use the following "special categories" of more sensitive personal data:

- Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences (where required and relevant to your role).

How is your personal data collected?

We collect personal data about candidates from the following sources:

- You, the candidate.
- Your recruitment agency or the recruitment agency that we have appointed for the purposes of filling the vacancy for which you are being considered, from which we collect the following categories of data: your CV and covering letter, your previous employment history, previous experience, skills, qualifications, name, address, contact details, referees and any other information relevant to the position (which in the case of more senior fee earning roles may include previous performance), including financial performance and a business case relating to what you anticipate delivering for us if you are successful in the recruitment process.
- We may collect additional information from third parties including former employers (information will only be collected from former employers in relation to reference checks and only after we have informed you that we will be taking up such references).
- If you are a solicitor, we will check the Solicitors Regulation Authority (SRA) and/or Law Society website to ensure that you are a solicitor and check that you have a practicing certificate free from restrictions to ensure that you can practice as a solicitor.

- Your named referees, from whom we will ask to provide us with a reference about you. This will generally include dates of employment, position held, reason for your employment ending (if it has), relevant experience and relevant performance assessment.
- We also carry out the following checks on all applicants:
 - Electronic verification and adverse media checks on new joiners (currently carried out via Zinc), to confirm your identity including (if applicable) right to work in the UK.
 - SRA section 43 restrictions check.
 - DBS checks on all new partners including salaried partners.

How we will use information about you

We will use the personal data we collect about you to:

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks, where applicable.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.
- Comply with legal or regulatory requirements.
- Make a decision about your recruitment or appointment.
- Determine the terms on which you work for us
- Check you are legally entitled to work in the UK.
- If you are applying to work in our Northampton, Leicester or Norwich offices, or attend our Northampton, Leicester or Norwich offices for interview, we have CCTV in operation at those offices. Broad details of our CCTV are below (and full details can be found in our CCTV policy):
 - At our Northampton office we have one camera that covers the entrance to our car park, giving a view of the barrier arm, key pad and intercom. A second camera covers the front entrance to our building and an area of the car park which is part of our demise
 - At our Norwich office, the CCTV monitors the main reception entrance (inner and outer doors), the entrance to the car park and the alleyway from the car park to the main road.

It primarily covers those visiting our offices (but is angled so as not to cover members of the public walking by) and cars entering our car park.

- At our Leicester office, the CCTV monitors the main entrance, the car park, and the full perimeter of the building. It primarily covers those visiting our offices (but is angled so as not to cover members of the public walking by) and cars entering our car park. Again, the CCTV operates for 24 hours a day, and this Data is continuously recorded.

Images from cameras can be viewed from the reception desk at the relevant office and in secure setting by authorised personal for a short period after (save if there is a legal basis for keeping footage long, such as in the event of a criminal investigation).

It is in our legitimate interests to decide whether to appoint you to role since it would be beneficial to our business to appoint someone to that role.

We also need to process your personal data to decide whether to enter into a contract of employment or engagement with you.

Having received your CV and covering letter, we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether your application is strong enough to invite you for an interview. 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 offer you the role.

If we decide to offer you the role, we will then take up references. If we offer you a role as a solicitor, this will be conditional on you being able to obtain a practising certificate from the Solicitors Regulation Authority (SRA) free from restrictions. As a result, we may need to obtain information from you regarding any spent or unspent convictions affecting you. This will need to be done before we can confirm your appointment.

If we are appointing you to a sensitive role within the Firm (which may include dealing with client accounts or client confidential information) we may be required to obtain information from you regarding spent or unspent criminal convictions.

If your employment is likely to involve you in undertaking work on any Government contracts, your employment will also be subject to your completion of a Baseline Personal Standard Security form, which contains a criminal conviction declaration form. It is a condition of our Government contracts that all new employees who are required to work on government contracts complete this form. Should this requirement change, we will let you know. Further information on this will be provided in the privacy notice that we issue to employees, workers and contractors if you are offered and accept a position with us.

If you fail to provide personal data

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we may not be able to process your application successfully. For example, if we require a credit check or references for this role and you fail to provide us with relevant details, we may not be able to take your application further.

How we use particularly sensitive personal data

“Special categories” of particularly sensitive personal data require higher levels of protection. This includes the following information: race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic/biometric data, health, sex life or sexual orientation.

We will use your particularly sensitive personal data 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 the interview or any assessment, or in the case of trainee solicitor applications in relation to the assessment centre or any tests undertaken.
- We will use information about your race or national or ethnic origin, religious, or philosophical beliefs, or your sex life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

Information about Criminal Convictions

We envisage that we may have to process information about criminal convictions, if relevant and if legally required taking into account the nature of the role you have applied for.

We are entitled 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.

We may collect information about your criminal convictions history in the case of solicitors to ensure that you meet, or continue to meet, the requirements of the SRA Suitability Test. In the case of solicitors we are required to obtain this information because the role of solicitor is listed as an Excepted Profession in Part 1, Schedule 1 of the Rehabilitation of Offenders Act (Exceptions) Order 1975 (as amended).

As stated above, your employment may also be subject to your completion of a Baseline Personal Standard Security form, which contains a criminal conviction declaration form in the event that you are likely to work on government contracts.

Whenever the Firm collects criminal conviction history it will ensure that it keeps such data securely and such information will be restricted only to those persons involved in making recruitment or suitability decisions.

Automated Decision-Making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

Data Sharing

Why might you share my personal data with third parties?

We will only share your personal data with the following third parties for the purposes of processing your application:

- your recruitment consultant or the recruitment consultant/search consultancy that we have appointed,
- if relevant the SRA,
- our applicant tracking system, currently the Eploy system provided by ITS Software Systems Ltd,
- our third party provider who conducts contextual analysis using your background information (only with your express consent), currently Rare Recruitment Limited,
- We will also make contact with your chosen referees and former employers but will indicate to you before we do this.

We may also from time to time use recruitment platforms to manage our vacancies, applications and/or recruitment process. In doing so your personal data will be shared with the relevant provider of the recruitment platform.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need-

to-know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

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

How long will you use my personal data for?

If you are unsuccessful in your application for employment (then save as set out below), we will retain your personal data for a period of 9 months after we have communicated our decision.

We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. After this period, unless you ask us to hold your personal data for longer, we will securely destroy your personal data in accordance with our data protection policy and any policies on retention of personal data.

If we wish to retain your personal data on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal data for a fixed period on that basis.

For successful candidates who accept the offer of employment or engagement with us, we will retain the recruitment data (CV, application form, interview assessments/notes etc) for the duration of your employment to the extent that it remains relevant to your employment (and possibly thereafter). Please see the privacy notice that we will issue to you as an employee for further information relating to this.

Rights of Access, Correction, Erasure, and Restriction

Your rights in connection with personal data

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

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. Please note that we may need to verify the accuracy of the new personal data that you provide.

- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data 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 data where you have exercised your right to object to processing (see below). Please note, however, that we may not always be able to comply with your request for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular 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 data for direct marketing purposes. In some cases we may demonstrate that we have compelling legitimate grounds to process your personal data which override your rights and freedoms.
- **Request the restriction of processing** of your personal data in certain circumstances. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to you or to another party. This right only applies to automated information for which you initially provided consent for us to use, or where we used the information to perform a contract with you.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to another party, please contact our People Manager (Natalie Clarke) in writing.

Right to Withdraw Consent

In the limited circumstances where we have relied on your consent for the collection, processing and transfer of your personal data for a specific purpose (which will be rare), you have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact our People Manager (Natalie Clarke). Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Data Protection Officer

We have appointed a data protection officer (DPO) to oversee compliance with this privacy notice. Our Data Protection Officer is Hannah Steggles, Partner. She can be contacted on 0116 2473520 or email dpo@howespercival.com. If you have any questions about this privacy notice or how we handle your personal data, please contact the Data Protection Officer.

Complaints

You have the right to make a complaint to the Information Commissioner at any time. However, we would appreciate the opportunity to deal with your complaint in the first instance. We have a data protection complaints policy, a copy of which can be found [here](#), which sets out how we will handle your complaint. If it is helpful, you can use our [data protection complaints form](#) to make a complaint. Whether or not you choose to make a complaint to us first, you still have the right, at any time to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

The Firm's Data Protection Officer is responsible for this Notice which was adopted on 8 May 2018 and last updated on 15 June 2026.