DATA PROTECTION PRIVACY NOTICE (EMPLOYMENT)

INSTITUTE OF BARRISTER'S CLERKS

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Who collects the information?

The Institute of Barrister's Clerks (the IBC) is a 'data controller' and gathers and uses certain information about you.

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our Data Protection Policy.

About the information we collect and hold

What information?

We may collect the following information during your employment:

- Your name, personal and work contact details (i.e. address, home and mobile phone numbers, email addresses) and emergency contacts (i.e. name, relationship and home and mobile phone numbers);
- Information collected during the recruitment process that we retain during your employment;
- Employment contract information;
- Details of salary and benefits, bank/building society, National Insurance and tax information, your age;
- Details of your spouse/partner and any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- [A copy of your driving licence;]
- [Details of your share incentive arrangements, and all information included in these and necessary to implement and administer them;]
- Details of your pension arrangements, and all information included in these and necessary to implement and administer them;

- Information regarding your fitness for work, and information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health);
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;
- [Criminal records information, including the results of Disclosure and Barring Service (DBS) checks;]
- [Your trade union membership;]
- Information on grievances raised by or involving you (depending on the nature of the grievance this may include sensitive personal information);
- Information on conduct and/or other disciplinary issues involving you (depending on the nature of the issue this may include sensitive personal information);
- Details of your appraisals and performance reviews;
- Details of your performance management/improvement plans (if any);
- Details of your time and attendance records;
- [Information regarding your work output;]
- Information in applications you make for other positions within our organisation;
- Information about your use of our IT, communication and other systems, and other monitoring information;
- Your image, in photographic [and video] form;
- Details of your use of business-related social media, such as LinkedIn;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and
- Details in references about you that we give to others.

Certain of the categories above may not apply to you if you are a worker, agency worker, independent contractor, freelancer, volunteer or intern.

How we collect the information

We may collect this information from you, your manager, your personnel records, the Home Office, [share scheme administrators,] [pension administrators,] your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, [the DBS,] [your trade union,] other employees, [consultants and other professionals we may engage, e.g. to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure,] [insert details of systems used e.g. door entry systems, swipe card systems, time management system,

time clock records, application logs,] [insert details of relevant systems, such as keystrokes and mouse movements, screen capture, application logs, webcams, [automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote access systems, [trading platforms,] email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records [insert any other relevant systems such as data loss prevention tools, next-generation firewalls, unified threat management systems, transport layer security, eDiscovery technology, mobile device management systems,] [relevant websites and applications].

Why we collect the information and how we use it

We will typically collect and use this information for the following purposes (other purposes that may also apply are explained in our Data Protection Policy [insert any other relevant policies]):

- for the performance of a contract with you, or to take steps to enter into a contract;
- for compliance with a legal obligation (e.g. our obligations to you as your employer under employment protection and health safety legislation, and under statutory codes of practice, such as those issued by Acas);
- for the purposes of our legitimate interests or those of a third party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.
- because it is necessary for carrying out obligations or exercising rights in employment law;
- for reasons of substantial public interest (i.e. equality of opportunity or treatment, [promoting or retaining racial and ethnic diversity at senior level,] [regulatory requirements]); and
- to defend any legal claims that may be brought against us in connection with your employment, or to establish, bring or pursue any claim against you, e.g. to enforce post-termination restrictions; this will typically involve passing information on to our legal advisers, who will be subject to strict professional and contractual duties of confidentiality.

Further information on the monitoring we undertake in the workplace and how we do this is available in our [insert details of relevant policy that deals with monitoring undertaken by the employer], available from [set out details of how employee can access the policy].

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

How we may share the information

We may also need to share some of the above categories of personal information with other parties, such as external contractors and our professional advisers and with potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information [with our regulators or] as required to comply with the law.

Where information may be held

Information may be held at our offices, and third-party agencies, service providers, representatives and agents as described above. [Information may be transferred internationally to [identify any particular country that is relevant] [and other countries around the world, including countries that do not have data protection laws equivalent to those in the UK, for the reasons described above.] We have security measures in place to seek to ensure that there is appropriate security for information we hold.

How long we keep your information

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed.

Your right to object to us processing your information

Where our processing of your information is based solely on our legitimate interests (or those of a third party), you have the right to object to that processing if you give us specific reasons why you are objecting, which are based on your particular situation. If you object, we can no longer process your information unless we can demonstrate legitimate grounds for the processing, which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.

Please contact [insert name and/or position of person responsible for data protection] who can be contacted [set out details of how named person can be contacted, e.g. email and telephone number] if you wish to object in this way.

Your rights to correct and access your information and to ask for it to be erased

Please contact [insert name and/or position of person responsible for data protection], who can be contacted [set out details of how named person can be contacted, e.g. email and telephone number] if (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask [insert name and/or position of person responsible for data protection] for some but not all of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. [insert name and/or position of person responsible for data protection] will provide you with further information about the right to be forgotten, if you ask for it.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

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

How to complain

We hope that [insert name and/or position of person responsible for data protection] can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.