

Data & Privacy Notice

Our Privacy Policy

This Notice is primarily for the benefit of our clients or potential clients or for related third parties whose data we may process as part of the provision of legal services. We maintain and will provide separate privacy notices in relation to the collection and use of personal information about our staff and employees, including potential employees, during and after their working relationship with us.

This firm processes your data in accordance with the terms of the Data (Use and Access) Act 2025, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019) and the relevant provisions relating to the General Data Protection Regulation contained within the European Union (Withdrawal) Act 2018 (UK GDPR).

The terms 'personal data', 'data controller', 'data processor' and 'data subject' are as defined in the Data Protection Act 2018 and UK GDPR.

This Data & Privacy Notice explains, in detail, the types of personal data we may collect about you when you interact with us. It also explains how we will store and handle that data and keep it safe. Unless otherwise indicated, references in this Data and Privacy Notice to the GDPR refer to the UK GDPR.

We know that there's a lot of information here, but we want you to be fully informed about your rights, and how our firm uses your data. We hope the following sections will answer any questions you have but if not, please do get in touch with us.

Conditions for Processing Data

We are only entitled to hold and process your data where the law allows us to. The current law on data protection (Article 6 GDPR) sets out a number of different reasons for which a law firm may collect and process your personal data. These include:

Contractual obligations

The main purpose for our holding your data is to provide you with legal services under the agreement we have with you. This agreement is a contract between us and the law allows us to process your data for the purposes of performing a contract (or for the steps necessary to enter into a contract).

Legitimate Interests

In specific situations, we require your data to pursue our legitimate interests in a way which might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests. This may include to satisfy our external quality auditors or our Regulators. Should we identify a need to use this processing basis, we will have ensured the our use of personal data is necessary for the purposes of the legitimate interests we have identified and that this processing has been balance against the interests of the data subject whose information we need to use.

Recognised Legitimate Interests

In some circumstances, we may need to process your data for the purposes that do not relate to our core functions but because there is a recognised legitimate interest and the data processing is in the public interest. This may include:

- processing of data necessary for national security, public security and defence purposes
- processing of data necessary for the detection, investigation or prevention of crime
- responding to data requests made by bodies acting in the public interest, for processing by those bodies for purposes laid down in law (for example, to help a government agency discharge its duties and functions), or
- processing of data necessary for the safeguarding of vulnerable individuals.

Where data processing is based on recognised legitimate interest, we would not need to conduct a legitimate interest assessment and you may not be able to ask us to stop this processing.

Legal compliance

If the law requires us to, we may need to collect and process your data. For example, we can pass on details of people involved in fraud or other criminal activity.

Consent

In some situations, we can collect and process your data with your consent. For example, when you tick a box to receive email newsletters. When collecting your personal data, we'll always make clear to you which data is necessary in connection with a particular service.

When do we collect your data?

We normally collect your data when you provide it to us or when it is provided to us by others (your opponent's solicitors for example) during your case. You may give us your data by email; through an online web form; over the telephone; face to face; or by post.

What sort of data do we collect?

Information you provide to us

You voluntarily give us your personal information for instance when:

- you contact us via our website
- provide a comment on our website
- write a review
- sign up to any newsletters
- interact with us on social media platforms, and/or
- use our services.

Where we request information from you we will collect the information set out in the relevant web pages, or as explained to you over the telephone or face to face.

Client services

We may collect personal data as follows:

- name and contact details (including address, email and phone numbers). This may include asking for and keeping a copy of your passport/driving licence and proof of address
- date of birth
- personal information that may be included in communications with us
- payment information and financial information that relates to a contractual relationship including bank details.

We may gather details of your age; ethnicity; gender etc.

We also collect and hold information about your case or legal problem.

We do not envisage that any data we hold would be classified as 'special categories' under the GDPR. If we need to start processing this type of data, or if we are acting as a Data Processor for this data then we will explain this to you.

Website or third party sources

We may sometimes collect certain related technical information including, but not limited to, traffic data, location data, logs (including, where available, the IP address and location of the device connecting to the online services and other technical information and identifiers about the device and the nature of the visit such as clickstream to, through and from our website) and other communication data, and the resources that you use.

Telephone call recording

We record most incoming and outgoing telephone calls with the exception of calls (or parts of those calls) where payment is taken. Your personal data may be collected as a result.

We record conversations for the following reasons:

- to allow us to be able to properly assess the needs of our clients (including potential clients) and third parties in order that we can provide them with a better service and resolve their queries
- to ensure we comply with regulatory requirements
- to identify training and development needs
- to identify and evaluate any expressions of dissatisfaction and/or complaints
- to enable us to review call quality
- to protect the wellbeing and safety of our staff by identifying any threatening behaviour which can then be evidenced and acted upon where necessary.

Call recordings are destroyed in accordance with the retention information in this Notice. If the recording is available, you can submit a request a copy of your call by making a data subject access request to our DPO (as set out below).

How do we use your data?

Provision of services

We only use your data for the purposes of providing you with legal advice, assistance and where appropriate, representation and for reasons directly associated with those services (i.e. providing information to quality auditors etc.).

In particular:

- to deliver our services
- to manage our relationship and communicate with you
- to provide you with advice or guidance about our services
- to make and manage payments
- to respond to complaints and seek to resolve them
- to train our staff and measure the quality of the service we give to clients.

Regulatory

We also use data to communicate with our regulators or legislators and to obey laws, regulations and codes of conduct that apply to us.

For example, we will process your data to enable us to identify and/or verify your identity and conduct fraud, credit and anti-money laundering checks in accordance with anti-money laundering and counter terrorism financing legislation and regulation.

Consent

We may use your data to notify you of our other services but only where we have your consent to do so.

Website enhancement and business development

We also use data to develop our business and services. In particular:

- to respond to individual experiences shared with us and for editorial content
- to enhance your online experience
- to conduct research and surveys
- to develop and manage our services including marketing of new or enhanced services
- to research your views and experiences for research and editorial purposes, including through requests for feedback on our services
- to understand your website journey, including what pages you have viewed and for how long
- to administer and keep safe and secure our website and for internal operations, including data analysis, testing, statistical purposes.

Cookies

A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyse web traffic or lets you know when you visit a particular site.

You can choose to accept or decline most cookies although some we are able to use without your consent. Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer. This may prevent you from taking full advantage of the website.

By law, some cookies such as those that collect data for statistical purposes and appearance cookies that adapt appearance of the website (such as by changing the language to suit your preferences), may be placed on your computer without your permission.

Other cookies may not be placed on your computer without your consent, unless they are strictly necessary to the operation of the service that we provide on the website.

The following table summarises the analytics cookies we use for our website:

Cookie	Provider	Purpose	Duration	Type
_ga	Google Analytics	Distinguishes users and helps measure website usage.	Up to 2 years	Analytics
ga*	Google Analytics	Maintains session state and interaction information.	Up to 2 years	Analytics
hjSessionUser*	Hotjar	Recognises returning visitors and associates their interactions with the same user.	Up to 1 year	Analytics
hjSession*	Hotjar	Maintains information about the visitor's current session and interactions.	Up to 1 day	Analytics

We use Google Analytics to monitor how our website is being used so we can make improvements. Our use of Google Analytics requires us to pass to Google your IP address (but no other information) – Google uses this information to prepare site usage reports for us, but Google may also share this information with other Google services. In particular, Google may use the data collected to contextualize and personalize the ads of its own advertising network. Related information:

- [Google's privacy policy](#)
- [How Google uses this information.](#)

If you have any queries about the cookies that we use, or would like more information, please contact david@humber.law.

Artificial Intelligence

In order to provide an optimum service to our clients, under the agreement we have with you to provide legal services, we may utilise technology which uses artificial intelligence (AI). In particular, we may use AI for the following:

- to improve our business processes such as by using AI to help extract, organise and compile documents, summarise text or extract data for entry into relevant systems
- to help with our marketing such as by creating posts and product information
- to expedite and improve our legal services such as for compiling court bundles, identifying content, legal research and extracting and analysing content within documents
- to help facilitate our anti money laundering, cyber security and fraud detection procedures

However, we aim to take steps to ensure that we remain fully accountable and our use of AI technology is safe, secure and compliant with data protection legislation as well as the professional rules that govern our work.

In addition to adhering to the data processing principles in the UK GDPR including fairness and accuracy, we also seek to evaluate and improve the 'statistical accuracy' of data generated by any AI system. Statistical accuracy refers to the accuracy of an AI system itself. Any AI system we use needs to be sufficiently statistically accurate to ensure that any personal data generated by it is processed lawfully and fairly.

In many cases, the outputs of an AI system are not intended to be treated as factual information about an individual. Instead, they are intended to represent a statistically informed guess as to something which may be true about the individual now or in the future. To avoid such personal data being misinterpreted as factual, we seek to ensure that the records generated by an AI tool indicate:

- wherever data outputs are statistically informed guesses rather than facts
- where possible, the provenance of the data and the AI system used to generate the inference
- where the inference was based on inaccurate data, or the AI system used to generate it is statistically flawed in a way which may have affected the quality of the inference
- if the processing of the incorrect inference may have an impact on an individual. If this applies, an individual affected it would be notified and may request the inclusion of additional information in their records to counter the incorrect inference.

Wherever possible, we will ensure any factors that may result in inaccuracies in personal data are corrected and the risk of errors is minimised.

We seek to apply enhanced and comprehensive security whenever AI is implemented. Personal data will only be processed through an AI tool where we have conducted a data protection impact assessment and are assured that we can put in place practical steps to mitigate any risks and adequately maintain and protect confidentiality and privacy.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are allowed to use automated decision-making without your consent provided that we implement appropriate safeguards including where we:

- provide you with information about the decision
- enable you to make representations about the decision
- enable you to obtain human intervention about the decision, and
- enable you to contest the decision.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

WhatsApp

Where all parties consent, we may use WhatsApp as a convenient way to communicate with clients and provide updates on their case.

While we strive to keep our communications secure and will keep WhatsApp messages confidential and only access them when necessary to provide our services, it is important to understand that WhatsApp messages, like other communications, are stored on client files for record-keeping and may potentially be used in the legal process.

Please be aware that WhatsApp operates its own [privacy policy](#), which we encourage you to read. We also encourage those who may engage with us via this platform to secure access to their devices and use up to date versions of the software for secure communication.

How do we protect your data?

We take protecting your data very seriously. The data you give us may be subject to Legal Professional Privilege and is often extremely sensitive and confidential.

With this in mind we will treat your data with the utmost care and take all appropriate steps to protect it. We have clear data protection and information security policies and procedures in place (along with Regulatory and other legal obligations to keep your data safe) and these are regularly assessed as part of our Quality Standards and compliance processes.

We protect our IT system from Cyber Attack. Access to your personal data is password-protected, and sensitive data is secured by encryption.

We regularly monitor our system for possible vulnerabilities and attacks, and we carry out penetration testing to identify ways to further strengthen security.

How long will we keep your data?

We only keep your data for as long as is necessary for the purpose(s) for which it was provided.

We use the following retention periods and review these periodically to make sure we are only keeping personal data and other data for as long as is needed:

- information in a matter file or related to a matter or instructions to us such as information on our case management system will usually be kept for a period of seven years after the case or matter ends unless it is required to be kept for longer (for instance, the information is required for another or related case or matter or where the person is currently under the age of eighteen, in which case data will need to be held for seven years after they reach the age of eighteen), or we have another legal basis to process that information. This is because we are required to keep client files for that period by our Regulator and/or by the SRA. This also protects you should you be unhappy with our services and want to complain or even sue us after your case ends.
- data obtained for compliance with crime or fraud prevention has to be retained by us to meet our legal or regulatory obligations for five years from the close of the individual matter or the end of our business relationship with a relevant person, whichever is later.
- enquiries where we do not take on your case are kept for only 18 months.
- any complaints files for seven years after the complaint is concluded (with the associated matter file(s)).
- financial information and any financial transactions will be kept for a period of seven years to comply with HMRC requirements except for cardholder data which will generally be destroyed immediately after the transaction is processed.
- enquiries about job opportunities and information relevant to recruitment (where a job offer is not made) are kept for 12 months. Information about retention of personal data collected and processed for as part of the recruitment process for successful applicants will be provided as part of that process.
- call recordings are stored in line with the above timescales, for instance for 7 years if the calls relate to a matter we have advised on.

For some data we may decide that it is proper and appropriate to keep data for longer than the above, but we will notify you if we believe that your case falls into this category or there is another reason your data has to be retained.

Who do we share your personal data with?

We sometimes share your personal data with trusted third parties. We only do this where it is necessary for providing you legal services or for the effective operation of our legal practice.

For example, we may share your data with barristers; experts; translators; costs draftsmen; process servers; secure file storage and destruction companies; auditors; the company that securely hosts our off-site cloud storage servers.

We apply a strict policy to those recipients or data processors to keep your data safe and protect your privacy. In particular:

- We provide only the information they need to perform their specific services
- They may only use your data for the exact purposes we specify in our contract with them
- We work closely with them to ensure that your privacy is respected and protected at all times
- If we stop using their services, any of your data held by them will either be deleted or rendered anonymous.

Where is your data processed?

We may transfer personal data overseas. In particular:

- we use cloud IT and similar data storage facilities and so we may store, process and transmit data in locations outside the UK;
- the firm's information systems, including electronic matter files, client information and finance systems are accessible by our offices in different countries which means personal data may be accessed by our firm's personnel overseas;
- where we need to perform pre-contractual measures (credit and identity checks) or because the checks we request are necessary for important reasons of public interest;
- where a client matter involves obtaining legal or other professional advice from another country, our firm may need to transfer details about the client matter, including personal data, to a third party in that country.

Whenever we transfer any data out of the UK, we ensure that the degree of protection afforded to it is not materially lower than in the UK and that there are appropriate safeguards in place governing the transfer and subsequent processing, in accordance with our internal processes and policies as well as regulatory and legal obligations. In particular, we ensure that at least one of the following safeguards is implemented:

- we will only transfer personal data to countries that have been deemed to provide an adequate level of protection for personal data by the UK in accordance with transfers approved by UK adequacy regulations, have appropriate safeguards or otherwise comply with EU GDPR transfer restrictions, as applicable
- where we use certain service providers, we may use specific contractual provisions which gives personal data the same protection it has within the UK and ensures a similar level of protection to the personal data as if it was processed within the UK, as applicable, and/or

- we will require that any overseas third party to which we disclose personal data to: (a) only use that personal data for the purposes for which it was disclosed (b) use all technical and organisational measures which are reasonable in the circumstances to secure that personal data (c) delete that personal data when it is no longer required, and (d) treat that personal data in accordance with this Data and Privacy Notice and that appropriate data privacy law.

What are your rights?

You have the following rights under the UK GDPR:

1. the right to be informed – the provision of clear and concise information about what we do with your personal data, as outlined within this Data & Privacy Notice
2. the right of access – commonly referred to as a ‘data subject access request’, this enables you to request a copy of your personal data to understand how and why we are using your data, and to check we are doing so lawfully. If we choose not to action your request, we will explain to you the reasons for our refusal
3. the right to rectification – the ability to have inaccurate personal data rectified or, in specific circumstances dependent on the purposes for our processing of your data, the ability to have incomplete personal data completed
4. the right to erasure – also known as the right to be forgotten, this permits you to request we erase your personal data. This only applies to data we hold at the time your request is received and does not apply to any data that may be obtained in the future. Please note that this is not an absolute right and only applies in certain circumstances. We may have overriding duties to retain some data which you cannot ask to be erased immediately or at all. For instance, once you become a client of our firm or you are an interested party in a case, we will be required by our regulators and for legal purposes to retain some of your personal data and other information within casefiles for a certain period (for retention periods, please see above)
5. the right to restrict processing – the ability to request a temporary restriction on the processing of your personal data, where one of a limited number of reasons specified by the Information Commissioner’s Office (ICO) applies
6. the right to data portability – the ability to receive personal data you have provided to us in a structured, commonly used and machine readable format. This also gives you the right to request that we transmit this data directly to another Data Controller
7. the right to object – the ability, in certain circumstances, to request we stop processing your personal data. This request may relate to all of your personal data we hold or only certain information, and may only apply to a particular purpose for processing
8. rights in relation to automated decision making and profiling – restrictions on the use of automated decision making and profiling where such decisions have a legal or similarly significant effect on you.

For further details on your rights, please visit the Information Commissioner’s Office at <https://ico.org.uk/your-data-matters/>.

Contact Details

For information on how your information is used, how we maintain the security of our information, and to exercise your rights to access information we hold on you, please contact us. Similarly, if you believe that the information we hold is wrong or out of date, please let us know and we will update it. The person in this firm responsible for data protection is our Data Protection Officer, David Stokes, and enquires and requests can be sent to them by telephone 01482 872739, by emailing

david@humber.law or in writing to Humber Law, Beverley Enterprise Centre, Beck View Road, Beverley, East Riding of Yorkshire HU17 0JT.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this policy. You should exercise caution and look at the privacy statement or policy applicable to the website in question.

Complaints about your personal data

In accordance with the Data (Use and Access) Act 2025, should you wish to raise a complaint about a potential breach of your personal data or if you have any other concern about our handling of your personal data, then, we have put in place the following steps to facilitate that process.

Should you wish to raise a complaint about a potential breach of your personal data or if you have any other concern about our handling of your personal data, please contact our Data Protection Officer (using the contact details provided above). They will acknowledge your complaint within 30 days and, without undue delay, take appropriate steps to respond to the complaint and inform you of the outcome.

In the event of an allegation of a breach of Personal Data and/or any concern that our firm has not handled your personal information properly, we will consider whether a report needs to be made to the ICO. Not all breaches are reportable and we will advise you of the results of our assessment.

You also have the right to lodge a complaint with the ICO. For further information or to contact the ICO please visit: <https://ico.org.uk/make-a-complaint/data-protection-complaints> or call 0303 123 1113.

The Regulator

If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us or complaint you made to us regarding the use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office. For further information or to contact the ICO please visit: <https://ico.org.uk/make-a-complaint/data-protection-complaints> or you can contact them by calling [0303 123 1113](tel:03031231113).

Alternatively, please go online to www.ico.org.uk/concerns (please note we can't be responsible for the content of external websites).

Changes to this Notice

We do not intend to process a client or related third party's personal information for any reason other than stated within this privacy notice. If this changes, we will update this privacy notice on this webpage and in any documentation we will send to you. However, internet and data privacy best practice and acceptable standards are developing. We therefore reserve the right to revise this Notice at any time. If this Notice changes in any way, we will place an updated version on this webpage. For all other clients with ongoing instructions, we will provide a copy directly. Continued instructions to us will signify that you agree to any such changes.

Version: 1.0 (30/09/2026)