

PRIVACY POLICY

This document, together with our Cookies Policy and our Terms of Business, set out what information Backhouse Jones Solicitors collects from visitors, clients and employees, how it uses the information, how it protects the information and your rights.

Backhouse Jones Solicitors is committed to ensuring your privacy is protected in accordance with Data Protection Standards.

Backhouse Jones Solicitors is using the following definition for Personal Data:

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts. <i>Personal data we gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job.</i>
Sensitive personal data	<i>Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data will only ever be carried out with the express permission of the individual.</i>

Backhouse Jones Solicitors may change this policy from time to time by updating this page. This policy is effective from 7th January 2021, but we ask you to check this page from time to time. Any updates or changes to the use of your personal data will be advised to you, prior to that change of use.

WHO ARE WE?

Backhouse Jones Solicitors is a specialist law firm providing legal advice and services to businesses operating within the transport sector. Our services include transport law, employment law, corporate and commercial legal services, and subscription-based legal support. We also deliver professional training, events, and provide service and product information, newsletters, articles, legal updates, and other publications. In addition, we process personal data in relation to the recruitment and employment of our own staff.

Our registered office is:

Backhouse Jones Solicitors
The Printworks
Hey Road

Clitheroe
Lancashire
BB7 9WD

CONTACT US

Website: <https://www.backhousejones.co.uk/>

Email: dataprotection@backhouses.co.uk

Phone: 01254 828 300

Post: Backhouse Jones Solicitors, The Printworks, Hey Road, Clitheroe, Lancashire BB7 9WD

For the purposes of all applicable data protection legislation, Backhouse Jones Limited is the data controller of your personal data. Backhouse Jones is registered with the Information Commissioner's Register of Data Controllers.

WHAT TYPES OF DATA DO WE COLLECT?

The information we collect will depend on the services we provide to you, the nature of our relationship with you, and the information you choose to provide. For example, we may collect personal data when you instruct us to provide legal services, register for training or events, subscribe to our newsletters or marketing communications, apply for employment with us, or otherwise interact with Backhouse Jones Solicitors.

Depending on the services we provide, we may collect one or more of the following categories of personal data:

- Identification and contact information, including your name, title, gender, marital status, postal address, billing or delivery address, email address, telephone number and, where relevant, next of kin details.
- Identity verification information, including copies of identification documents such as passports, driving licences, immigration documentation and other documents required to verify your identity.
- Financial information, including bank account details, payment card information, tax and National Insurance details, credit information and other financial data where required.
- Employment information, including your CV, employment history, qualifications, training records and references where relevant.
- Website and technical information, including your IP address, browser type and version, operating system, device information, cookies, login information and geographical location data collected when you use our website.
- Health information, where necessary to protect you, our clients or our staff, or where required as part of an employment relationship or to provide employment-related benefits. We will only process health information where there is a lawful basis for doing so.
- Criminal offence data, where required to carry out enhanced background checks, regulatory requirements or legal services on your behalf. Such information will only be processed where permitted by law.
- Legal matter information, including any personal information you provide to us in connection with legal advice or services that we are instructed to provide.
- Transaction information, including details of payments made to or received from you and records of services or products you have purchased from us.
- Profile information, including your preferences, interests, feedback, survey responses and information about how you use our services.
- Usage information, including details of how you interact with our website, products and services.
- Marketing and communication preferences, including your preferences for receiving marketing communications from us and your preferred methods of contact.

In certain circumstances, we may also process special category personal data, such as information relating to your health, racial or ethnic origin, religious beliefs or other sensitive personal information where this is necessary for the provision of our services, compliance with our legal obligations, or where you have given your explicit consent where required.

We may also collect information relating to your legal status, including information about your authority to act, or the authority of individuals acting on your behalf, where this is necessary for the legal services we provide.

COLLECTING PERSONAL DATA

When we collect personal data, our Privacy Notice (on this website) details:

1. Who we are
2. What personal information we are collecting
3. Why we need it
4. Legal Basis under which we are processing (typically 'Consent', 'Contractual Obligations' and/or 'Legitimate Interest') (<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-bases-for-processing/>)
5. What we are going to use it for and any decisions (automated or human) that it will be used for
6. Who that information will be shared with
7. The safeguards we have put in place to protect your information
8. Our standard retention period or legal need to retain that information

The types of personal data we may collect include:

- Personal identification data, such as your name, address, passport details, immigration status and banking information where required.
- Special category personal data, such as health, medical, wellbeing, religious or racial and ethnic information, where there is a lawful basis for processing this information.
- Legal status information, including details of your legal position in relation to the services we are providing and/or information relating to individuals who have authority to act on your behalf.

Further information about the lawful bases for processing personal data can be found on the Information Commissioner's Office (ICO) website.

HOW WE COLLECT PERSONAL DATA

Depending on the nature of our relationship with you and the services we provide, we may collect personal data in a variety of ways.

We may collect personal information directly from you when you provide it to us, including where:

- if you apply to become an employee of this firm, to allow us to process your application
- as an employee to allow us to administer our HR policy
- following your request to use our services or marketing
- by subscribing to our publications or attending our seminars or training courses
- to provide us with feedback
- if you want to become a supplier to us, to allow performance of the contract with you

We may collect this information from third parties or public sources such as: relatives, health care professionals (if you come to us via a health provider such as the NHS or Social Services) or online verification search providers.

WHAT WE USE YOUR PERSONAL DATA FOR

The specific use of personal data will be detailed in the relevant Privacy Policy for the specific service(s) we are providing you.

Purpose	Type of Data	Lawful Basis for Processing/Legitimate
To register you as a new client which will include: - checking your identity (Money Laundering Regulations) - checking your credit rating	Identity Contact Financial	- Performance of our contract with you - Necessary to comply with a legal obligation - Necessary for our legitimate interests
Delivering our services to you which will include: - managing payments/fees/charges - collecting/recovering monies owed to us	Identity Contact Legal Matter Transaction	- Performance of a contract with you - Necessary for our legitimate interests (recover debts owed to us) - Necessary to establish, issue or defend legal claims - Consent
To determine our services which will include: - improve our service - resolve complaints - monitoring & recording - telephone enquiries	Legal Matter Contact Technical Usage Profile Marketing	- Consent - Necessary for our legitimate interests (develop our range of products & services)
To manage our relationship with you, this includes: - telling you about changes to our Terms of Business/Privacy Policy - asking you to complete a survey/feedback form - asking you to leave a review/write a testimonial	Identity Contact Profile Marketing	- Performance of a contract with you - Necessary to comply with a legal obligation - Necessary for our legitimate interests (keep our records up to date/awareness of how clients use our services)
To allow you to use our extra services to include: - seminars - events - complete a survey	Identity Contact Profile Usage Marketing	- Performance of a contract with you - Necessary for our legitimate interests (develop our products & services, grow our business by observing how our clients interact with us)

To administer & protect our business, including our website (this includes: • testing & maintenance of our systems • support • hosting data • support • troubleshooting	Identity Contact Technical	• Necessary for our legitimate interests (provide IT systems/network security/prevent fraud/business organisation/smooth running of business) • Necessary to comply with a legal obligation
To suggest goods and services which may be of interest or may help you.	Identity Contact Technical Usage Profile	• Necessary for our legitimate interests (develop our products & services, grow our business)
Delivery of useful website content and advertisements to you to measure and understand how effective our services are.	Identity Contact Profile Usage Marketing	• Necessary for our legitimate interests (develop our products & services, grow our business by observing how our clients interact with us)
To use data analytics to improve our: • website • products & services • marketing • customer experience	Technical Usage Marketing	• Necessary for our legitimate interests (link customers to our products & services, keep the information we provide update & relevant, develop our business and marketing strategy)
To recruit new employees and employ staff • checking your identity • checking your professional qualifications • processing job applications • maintaining HR records • maintaining payroll records	Identity Contact Financial	• Performance of our contract with you • Necessary to comply with a legal obligation • Necessary for our legitimate interests

This list is not exhaustive but designed to provide you indicative uses of your personal data. Please ensure you read the appropriate Privacy Policy for the product or service we are providing you for specific information.

RETENTION OF DATA

We will retain your personal data for different periods depending on our relationship with you.

Retention schedule

Client	Retention Period
Identity documents	While the file is open and for 7 years
Client account records	While the file is open and for 7 years
Client file, including electronic held data, e.g. emails	While the file is open and for 7 years for files save for commercial or residential property & commercial transactions which are retained while the file is open and for 15 years
Client is a minor	While the file is open and for 7 years or until the minor reaches 18 years of age, whichever is the later
Basic client details (name)	Indefinitely (for conflict checking purposes), any personal data will be retained until you unsubscribe and no longer wish to receive our marketing materials (for marketing purposes)
Notarial clients	Personal data is retained in accordance with our Notarial Privacy Policy

Any other personal data held for marketing purposes	Any personal data will be retained until you unsubscribe and no longer wish to receive our marketing materials
---	--

Prospect	Retention Period
Any personal data we hold	Personal data will be retained until you unsubscribe and no longer wish to receive our marketing materials.

Suppliers	Retention Period
Any personal data we hold	Appropriate personal data will be held for the duration of the contract and for 7 years.

Recruitment	Document Type	Retention Period
Speculative job applications/work experience applications – unsuccessful	CV, covering letter	Immediately disposed of
Work experience	CV, covering letter, notes of interview	While work experience continues and for 12 months.
Recruitment records	Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may	Three months after notifying unsuccessful candidates of the outcome of the recruitment exercise. Successful applicants – while employment

	be transferred to a successful candidate's employment file). Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship).	continues and for seven years.
Employees	Personal data is retained in accordance with our Employee Privacy Policy.	

Links to other sites

We may provide, from time to time, links to other sites (including Back Academy Limited and other associated companies) via our email marketing, newsletter, blog article or other web links.

Because we have no control over these sites, we cannot take responsibility for the practise they may undertake in respect of privacy and/or protecting your Personal Data. We would therefore advise you to satisfy yourselves that these sites are operating privacy policies that inform you how they handle and protect your data – as we cannot take any responsibility for this.

Social media widgets and links

You are probably familiar with the Facebook “Like” button and the various “Share” buttons that are available to users of the internet.

We sometimes use these to allow us to promote our services to other people as well as get feedback as to what articles, pages or blogs are of interest.

These other service providers may collect Personal Data about you, such as IP address, pages you visit on our site and may set their own cookies to enable them to function properly. In much the same way as *Links to other sites* do not allow us to enforce our policies, we would suggest that you undertake the same checks regarding the privacy policy of the company providing those features.

Marketing subscription

If you have opted in to our Marketing, you can find the related privacy notice [here](#).

Third parties – Service providers, business partners and others

We work with several third-party services providers who undertake services for us, these include:

Service Provider or Provider Type	Service Provided to us or You
-----------------------------------	-------------------------------

Credit agency and anti-fraud services	To comply with our legal duties and/or to assess your ability to fund services from us we may need to engage third parties in relation to fraud and credit checking. This will be based on compliance with the law or standards our organisation must adhere to or, in the case of credit checking, our legitimate business interest.
GP, medical assessment, occupational health	Potentially to assess your ability to work for us or to process a claim on your behalf. Where there is a claim related to accidents or incidents affected the health or physical ability of an individual, we may need to share or review such health data to deal with the case. This may also be necessary to protect other staff or our customers. These instances may be the result of acting on your behalf or in defence of another party. The specific legal basis could therefore be: Contractual Obligation, Protecting the vital interests of an individual data subject, or legal obligations such as sharing within the legal process of dealing with a claim.
Your previous employer or references	Provision of feedback on your previous roles or you as an individual, this based on our legitimate interests.
Professional Bodies (including DBS) and Certification Boards	To ensure that you have the necessary professional certifications required for us to employ you and for any ongoing sector specific requirements of professional competence. This based on our legitimate interests but may also be to ensure we are complying with the law or industry regulations when undertaking work on behalf of clients.
Health, life insurance bodies as well as other in-service benefits	If you travel on business and/or are entitled to private medical or life insurance, we are required to pass on certain information to the companies that provide these services on our behalf. This is based on our contractual obligations with you as set out in your current contract or benefits package.

In most cases you will be made aware of the parties that we share information with, prior to us sharing this information.

HOW WE DISPOSE OF YOUR DATA

All personal data disposed of by us is done so in a secure manner. Paper based files are securely shred and electronic copies of information will be permanently deleted from our system, where this is not possible, we will endeavour to ensure the personal data is securely locked so that access cannot be gained.

Where we may share your information without your explicit consent.

We may be required or chose to share your information in certain circumstances without obtaining your explicit consent, some examples of this would be:

- To comply with any legal process, applicable law or governmental request e.g. warrant, summons, statutory reporting, court documents, sharing of evidence, sector specific compliance etc.
- To enforce/administer our agreements
- To protect your vital interests in the event you are unable to provide your consent
- To protect our company or the public from harm or illegal activities
- For fraud prevention, investigation, risk assessment

- To protect the rights and property of our company
- To defend ourselves against third-party claims or allegations
- To protect the rights or freedoms of other data subjects

In any event, we will consider your rights and privileges before sharing this information.

YOUR RIGHTS

How you can help protect your personal data

In all cases, the information we require to obtain for you is necessary in the provision or assessment of the provision of services to you. We rely on this information being accurate and up to date, which is in part our responsibility as well as yours.

We only record information relevant to the provision of the service we are delivering to you. However, in many cases you can limit the use of your information for services that do not require your data e.g. you can opt-out of receiving our newsletter.

CHANGES TO YOUR PERSONAL DATA

In the event that your Personal Data, that we use to provide you goods or services, changes e.g. your surname, address, email address or Sensitive Personal Data E.g. Religion, Health Data – it is critical that you inform us of these changes to ensure we have the correct information on our systems. Where you have access to administer these changes yourself, we would expect you, if you are able, to update these details accordingly or else inform us of changes as soon as possible.

You should inform us in writing, by email, by telephone or in person – however we may also need to undertake further identity verification depending on the nature of the requested update.

COOKIES

Cookies are small files that are downloaded by many web sites to either enable a site to work, to assist you e.g. remembering your username and/or passwords, to track your behaviour to show relevant content and to show relevant marketing information which in turn may follow you across other sites.

You can opt-out of allowing cookies by instructing your browser to stop accepting cookies or to prompt you before accepting a cookie from a website you visit, by changing the settings within your browser software.

For specific information on how we use cookies on our website, please see our [Cookie Policy](#).

MAILING LIST OPT-IN – MARKETING EMAILS & NEWSLETTERS

You may opt-out of receiving marketing emails and newsletters from us by using the unsubscribe link within each email or contacting us directly.

Opting out of marketing lists, only removes you from such communication. Transactional emails e.g. those relating to services we are providing to you or responding to queries or enquires you make to us, may still result in us emailing you information where that medium is most appropriate.

SECURITY

Backhouse Jones Solicitors operates against a Privacy by Design and By Default policy. This means that before we use your data, we have already considered the potential impact on you were your data to be lost, stolen, shared or compromised.

We undertake routine reviews of our processes and security policies to ensure that we can take all reasonable precautions in protecting your data.

Where at all possible we encrypt all information that is either stored or transmitted to third parties. Where data is stored or transmitted to a Third Country, we will ensure appropriate adequacy protection is in place in accordance with Data Protection Legislation.

Consequently, we may also need to sometimes undertake further security and screening questions when undertaking our routine dealings with you these are there to protect your personal data and security.

Whilst we undertake all reasonable precautions, encryption, software updates and patches, we cannot guarantee the safety of data transmitted over the internet.

DATA BREACH

In the event of a data breach of your personal data, which means: "The unintended loss, destruction amendment or disclosure of personal data".

We will first do all that is necessary to minimise the impact on you, identify any potential malicious third-party, identify any third parties that may also be impacted and take all reasonable efforts to ensure that you are notified.

If we are notified by a third-party of a breach, in their systems, we will undertake the same level of efforts.

We will undertake this communication either directly with you as an individual or by sending out a public notification.

At the same time, we will comply with the current law in respect of informing the appropriate Supervisory Authority which is currently the Information Commissioners Office (ICO). We are under a

legal requirement to report Data Breaches to the ICO & our Regulatory Authority, the Solicitors Regulatory Authority (SRA).

CHANGES TO THIS POLICY

This policy may change at any time. You should review this page regularly, so you are aware of any changes. Substantial changes will be notified by a notice on our website.