

Morecrofts LLP

Privacy policy

We take your privacy very seriously. Please read this privacy policy carefully as it contains important information on who we are and how and why we collect, store, use and share your personal data. It also explains your rights in relation to your personal data and how to contact us or supervisory authorities in the event you have a complaint.

When we use your personal data, we are regulated by the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable UK data protection legislation. Morecrofts LLP acts as a data controller in respect of the personal data covered by this Privacy Policy.

Our use of your personal data is subject to your instructions, the UK GDPR, the Data Protection Act 2018 and other applicable legislation.

Key terms

It would be helpful to start by explaining some key terms used in this policy:

We, us, our	These expressions refer through the document to Morecrofts LLP, commonly referred to as Morecrofts
Our Information Compliance Manager	Our Information Compliance Manager is Julie Johnson who can be contacted at our Liverpool City Centre office or by email jj@morecrofts.co.uk
Personal data	Any information relating to an identified or identifiable individual
Special category personal data	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership Genetic and biometric data Data concerning health, sex life or sexual orientation

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.

Personal data we collect about you:

The table below sets out the personal data we will or may collect in the course of advising and/or acting for you.

Personal data we will collect	Personal data we may collect depending on why you have instructed us
Your name, address and telephone number Information to enable us to check and verify your identity, e.g. your date of birth or passport details Electronic contact details, e.g. your email address and mobile phone number Information relating to the matter in which you are seeking our advice or representation Information to enable us to undertake a credit or other financial checks on you Your financial details so far as relevant to your instructions, e.g. the source of your funds if you are instructing on a purchase transaction; or income and expenditure details to enable us to assess your eligibility for public funding	Your National Insurance and tax details Your bank and/or building society details Details of your professional online presence, e.g. LinkedIn profile Details of your spouse/partner and dependants or other family members, e.g. if you instruct us on a family matter or a will Your employment status and details including salary and benefits, e.g. if you instruct us on a matter related to your employment or in which your employment status or income is relevant such as determining eligibility for funding or exemptions from payment of fees. Your nationality and immigration status and information from related documents, such as your passport or other identification, and immigration information, if you instruct us on a matter to which this is relevant Details of your pension arrangements, e.g. if you instruct us in relation to financial arrangements following breakdown of a relationship Your employment records including, where relevant, records relating to sickness and attendance, performance, disciplinary, conduct and grievances (including relevant special category personal data), e.g. if you instruct us on matters related to your employment or in which your employment records are relevant Your racial or ethnic origin, gender and sexual orientation, religious or similar beliefs, e.g. if you instruct us on a discrimination claim Your trade union membership, e.g. if you instruct us on discrimination claim or your matter is funded by a trade union Personal identifying information, such as your hair or eye colour or your parents' names, e.g. if you instruct us to incorporate a company for you Your medical records, e.g. if we are acting for you in a personal injury claim or a family matter where they are required. Your social services records, e.g. if you instruct us in relation to a family matter or compensation claim in relation to that. Police records e.g. in some family or Personal Injury

Personal data we will collect	Personal data we may collect depending on why you have instructed us
	matters Financial details relevant to completion of tax returns and other documents, e.g. in trust matters. Financial documents in relation to your assets, income and expenditure, and general affairs, e.g. where we act for you in matrimonial proceedings.

This personal data is required to enable us to provide our service to you. If you do not provide personal data we ask for, it may delay or prevent us from providing services to you.

How your personal data is collected

We collect most of this information from you communicating with us directly in person or online. However, we may also collect information:

- from publicly accessible sources, e.g. Companies House, the Bankruptcy & Insolvency register, or HM Land Registry;
- directly from a third party, e.g.:
 - sanctions screening providers;
 - credit reference agencies;
 - client due diligence providers;
- from a third party with your consent, the list below is not exclusive but includes e.g.:
 - your bank or building society, another financial institution or advisor;
 - consultants and other professionals we may engage in relation to your matter;
 - your employer and/or trade union, professional body or pension administrators;
 - your doctors, medical and occupational health professionals;
 - Local Authorities
- via our website—we use cookies on our website (for more information on cookies, please see our cookies policy <https://www.morecrofts.co.uk/cookies/>)
- via our information technology (IT) systems, e.g.:
 - case management, document management and time recording systems;
 - automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, email, text and instant messaging systems;

CCTV Monitoring and Systems

- Morecrofts LLP operates CCTV systems at its offices, including reception areas and other parts of its premises.
- CCTV images may capture clients, visitors, contractors, staff, job applicants and other individuals attending our offices.

Why We Use CCTV

We use CCTV footage for the following purposes:

- Preventing and detecting crime.
- Protecting the safety and security of staff, clients and visitors.
- Protecting our premises, equipment, business property and assets.
- Maintaining a safe and secure working environment.
- Investigating health and safety incidents.

- Investigating security incidents.
- Investigating breaches of company policies or procedures where appropriate.
- Investigating allegations of misconduct where appropriate.
- Supporting legal claims, regulatory investigations or insurance matters where necessary.
- Client confidentiality will be respected at all times when CCTV footage is reviewed or disclosed. These purposes reflect the uses set out in our reception CCTV notice.

Lawful Basis for Processing CCTV Footage

We process CCTV footage under:

- Article 6(1)(f) UK GDPR, namely our legitimate interests in protecting our staff, clients, visitors, premises and business assets and maintaining security.
- Article 6(1)(c) UK GDPR where processing is necessary to comply with legal obligations.
- Where special category personal data is inadvertently captured by CCTV, it will only be processed where permitted under applicable data protection legislation.

Access to CCTV Footage

Access to CCTV recordings is restricted to authorised personnel who have a legitimate business need to access the footage.

Footage may be shared with:

- Law enforcement agencies.
- Regulatory authorities.
- Insurers and legal advisers.
- Other parties where disclosure is required or permitted by law.
- CCTV recordings are securely stored and protected against unauthorised access. This reflects the information provided within our CCTV reception notice.

CCTV Retention

- CCTV recordings will only be retained for as long as necessary to fulfil the purposes for which they were collected.
- Routine CCTV recordings are normally retained for 90 days, unless required in connection with:
 - an investigation;
 - a complaint;
 - disciplinary proceedings;
 - legal proceedings;
 - an insurance claim; or
 - a regulatory inquiry.
- Once no longer required, recordings will be securely deleted.

How and why we use your personal data

Under data protection law, we can only use your personal data if we have a proper reason for doing so, e.g.:

- to comply with our legal and regulatory obligations;
- for the performance of our contract with you or to take steps at your request before entering into a contract;

- for our legitimate interests or those of a third party; or
- where you have given consent.

A legitimate interest is when we have a business or commercial reason to use your information, so long as this is not overridden by your own rights and interests.

The table below explains what we use (process) your personal data for and our reasons for doing so:

What we use your personal data for	Our reasons
To provide legal services to you	For the performance of our contract with you or to take steps at your request before entering into a contract.
Conducting checks to identify our clients and verify their identity Screening for financial and other sanctions or embargoes Other processing necessary to comply with professional, legal and regulatory obligations that apply to our business, e.g. under health and safety regulation or rules issued by our professional regulator	To comply with our legal and regulatory obligations.
Gathering and providing information required by or relating to audits, enquiries or investigations by regulatory bodies	To comply with our legal and regulatory obligations.
Ensuring business policies are adhered to, e.g. policies covering security and internet use	For our legitimate interests or those of a third party, i.e. to make sure we are following our own internal procedures so we can deliver the best service to you.
Operational reasons, such as improving efficiency, training and quality control	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service for you at the best price
Ensuring the confidentiality of commercially sensitive information	For our legitimate interests or those of a third party, i.e. to protect our intellectual property and other commercially valuable information To comply with our legal and regulatory obligations.
Statistical analysis to help us manage our practice, e.g. in relation to our financial performance, client base, work type or other efficiency measures	For our legitimate interests or those of a third party, i.e. to be as efficient as we can so we can deliver the best service for you at the best price.
Preventing unauthorised access and modifications to systems	For our legitimate interests or those of a third party, i.e. to prevent and detect criminal activity that could be damaging for us and for you To comply with our legal and regulatory obligations.
Updating and enhancing client records	For the performance of our contract with you or to take steps at your request before entering into a contract To comply with our legal and regulatory obligations For our legitimate interests or those of a third

What we use your personal data for	Our reasons
	party, e.g. making sure that we can keep in touch with our clients about existing and new services.
Statutory returns	To comply with our legal and regulatory obligations.
Ensuring safe working practices, staff administration and assessments	To comply with our legal and regulatory obligations For our legitimate interests or those of a third party, e.g. to make sure we are following our own internal procedures and working efficiently so we can deliver the best service to you.
Marketing our services to: —existing and former clients; —third parties who have previously expressed an interest in our services; —third parties with whom we have had no previous dealings.	For our legitimate interests or those of a third party, i.e. to promote our business to existing and former clients.
Credit reference checks via external credit reference agencies.	For our legitimate interests or a those of a third party, i.e. for credit control and to ensure our clients are likely to be able to pay for our services.
High Court Enforcement and Enquiry Agents.	For the purpose of ensuring that any outstanding payments due to us are recovered.
External audits and quality checks, e.g. for Lexcel, ISO CQS or other accreditations and the audit of our accounts	For our legitimate interests or a those of a third party, i.e. to maintain our accreditations so we can demonstrate we operate at the highest standards To comply with our legal and regulatory obligations.
Special category personal data.	Where we process special category personal data, we will do so only where permitted under applicable data protection legislation and where an appropriate lawful condition for processing applies.
Maintaining office security, protecting staff, clients and visitors, investigating incidents and preventing crime through CCTV systems	Legitimate interests and legal obligations.

Promotional communications

We may use your personal data to send you updates (by email, text message, telephone or post) about legal developments that might be of interest to you and/or information about our services, including exclusive offers, promotions or new services or products.

We have a legitimate interest in processing your personal data for promotional purposes (see above '**How and why we use your personal data**'). This means we do not usually need your consent to send you promotional communications. However, where consent is needed, we will ask for this consent separately and clearly.

We will always treat your personal data with the utmost respect and never sell or share it with other organisations for marketing purposes.

You have the right to opt out of receiving promotional communications at any time by:

- contacting us by email to mail@morecrofts.co.uk or by telephoning 0151 236 8871 and speaking to a member of our marketing team
- using the 'unsubscribe' link in emails or 'STOP' number in texts

We may ask you to confirm or update your marketing preferences if you instruct us to provide further services in the future, or if there are changes in the law, regulation, or the structure of our business.

Who we share your personal data with

We routinely share personal data with:

- professional advisers who we instruct on your behalf or refer you to, e.g. barristers, medical professionals, accountants, tax advisors or other experts;
- other third parties where necessary to carry out your instructions, e.g. your mortgage provider, or HM Land Registry in the case of a property transaction, or Companies House;
- credit reference agencies;
- Enquiry agents and High Court Enforcement Officers;
- our insurers and brokers;
- external auditors, e.g. in relation to Lexcel or CQS or other accreditations and the audit of our accounts;
- our professional regulators
- The Legal Aid Agency, in cases where you are eligible for public funding (Legal Aid)
- our banks;
- external service suppliers, representatives and agents that we use to make our business more efficient, e.g. typing services, marketing agencies, document collation or analysis suppliers;

We only allow our service providers to handle your personal data if we are satisfied they take appropriate measures to protect your personal data. We also impose contractual obligations on service providers to ensure they can only use your personal data to provide services to us and to you.

We may disclose and exchange information with law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations.

CCTV footage may be disclosed to law enforcement agencies, regulatory authorities, insurers, legal advisers and other authorised third parties where necessary for the prevention and detection of crime, the investigation of incidents, legal proceedings, or compliance with legal obligations.

We may also need to share some personal data with other parties, say if there were potential buyers of some or all of our business or during a merger or 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 will not share your personal data with any other third party.

Where your personal data is held

Information may be held at our offices and those of third party agencies, service providers, representatives and agents as described above (see '**Who we share your personal data with**').

Some of our service providers may be based outside the United Kingdom. Further information about international transfers is set out below under 'Transferring Your Personal Data Internationally'."

How long your personal data will be kept

We will keep your personal data after we have finished advising or acting for you. We will do so for one of these reasons:

- to respond to any questions, complaints or claims made by you or on your behalf;
- to show that we treated you fairly;
- to keep records required by law.

We will not retain your data for longer than necessary for the purposes set out in this policy.

Different retention periods apply for different types of data. Further details on how long we will keep your data for will be provided to you when your file is closed and sent for storage. We may retain your electronic data for a longer period of time than any paper files.

When it is no longer necessary to retain your personal data, we will delete or anonymise it.

Transferring Your Personal Data Internationally

To deliver services to you, it may sometimes be necessary for us to transfer personal data outside the United Kingdom.

Where we do so, we will ensure that appropriate safeguards are in place in accordance with UK GDPR and applicable data protection legislation, including the use of approved international data transfer mechanisms where required.

Applying to us for employment

- 1.1 If you apply to us for a job, or for temporary and agency work, interns, volunteers and apprentices, then we will need to collect personal data,

We may collect personal data about you from various sources including:

- You, the candidate.
- Any recruitment agency through whom you have applied for the role
- A background check provider
- A credit reference agency
- Disclosure and Barring Service in respect of criminal convictions.
- Your named referees or other third parties whom you might ask us to approach
- A responsible adult with parental responsibility if you are under 18 years old.

About the information we collect and hold

We collect and hold the information up to and including the shortlisting stage of the recruitment process, to review your suitability for the role you have applied for and to complete our vetting and checking processes to ascertain information required by us and anything else required by law or our regulators. We may collect further information before making our final decision to recruit, i.e. before making an offer of employment unconditional.

We will not share any of this data with any third parties other than any information required to search the SRA or other professional databases, or to process a DBS check.

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

How long we keep your information

We keep the personal information that we obtain about you during the recruitment process for no longer than is necessary for the purposes for which it is processed. How long we keep your information will depend on whether your application is successful and you become employed by us, the nature of the information concerned and the purposes for which it is processed.

We will keep recruitment information (including interview notes) for no longer than is reasonable, taking into account the limitation periods for potential claims such as race or sex discrimination (as extended to take account of early conciliation), after which they will be destroyed. If there is a clear business reason for keeping recruitment records for longer than the recruitment period, we may do so but will first consider whether the records can be anonymised, and the longer period for which they will be kept.

If your application is successful, we will keep only the recruitment information that is necessary in relation to your employment. For further information, see our data protection privacy notice (employment).

Your rights

You have the following rights, which you can exercise free of charge:

Access	The right to be provided with a copy of your personal data
Rectification	The right to require us to correct any mistakes in your personal data
To be forgotten	The right to require us to delete your personal data—in certain situations
Restriction of processing	The right to require us to restrict processing of your personal data—in certain circumstances, e.g. if you contest the accuracy of the data
Data portability	The right to receive the personal data you provided to us, in a structured, commonly used and machine-readable format and/or transmit that data to a third party—in certain situations
To object	The right to object: —at any time to your personal data being processed for direct marketing (including profiling); —in certain other situations to our continued processing of your personal data, e.g. processing carried out for the purpose of our legitimate interests.
Not to be subject to automated individual decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal effects concerning you or similarly significantly affects you
CCTV Subject Access Requests	Where you can be identified in CCTV footage, you may request access to your personal data by making a Subject Access Request. We may need additional information to locate the relevant footage and verify your identity. Access may be restricted where disclosure would adversely affect the rights and freedoms of other individuals or where an exemption under data protection legislation applies.

For further information on each of those rights, including the circumstances in which they apply, please contact us or see the Guidance from the UK Information Commissioner's Office (ICO) on GDPR and data protection rights. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights>

If you would like to exercise any of those rights, please:

- email, call or write to our Information Compliance Manager—see below: ‘**How to contact us**’; and
- let us have enough information to identify you (*e.g. your full name, address and client or matter reference number*);
- let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill); and
- let us know what right you want to exercise and the information to which your request relates.

Keeping your personal data secure

We have appropriate security measures to prevent personal data from being accidentally lost, or used or accessed unlawfully. We limit access to your personal data to those who have a genuine business need to access 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.

If you want detailed information from Get Safe Online on how to protect your information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

How to complain

We hope that our Information Compliance Manager can resolve any query or concern you may raise about our use of your information.

You have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you are concerned about the way we have handled your personal data.

The Information Commissioner may be contacted at <https://ico.org.uk/concerns> or telephone: 0303 123 1113.

Changes to this privacy policy

We may update this Privacy Policy from time to time to reflect changes in legal requirements, regulatory guidance, business operations or data processing activities.

Where material changes are made, we will publish the updated version on our website and, where appropriate, notify clients and other affected individuals.

How to contact us

Please contact us and/or our Information Compliance Manager by post, email or telephone if you have any questions about this privacy policy or the information we hold about you.

Our contact details are shown below:

Our contact details	Our Information Compliance Manager's contact details
Morecrofts LLP Email mail@morecrofts.co.uk Telephone: 0151 236 8871	Julie Johnson Morecrofts LLP Cotton Exchange Old Hall Street, Liverpool L3 9LQ Email : jj@morecrofts.co.uk Telephone: 0151 236 8871

DOCUMENT CONTROL

Item	Detail
Policy Owner	Information Compliance Manager
Approved By	Partners
Version	2026.1
Effective Date	01.09.2026
Review Date	01.09.2027
Next Review	Annually or following regulatory change

Do you need extra help?

If you would like this policy in another format (for example audio, large print, braille) please contact us (see 'How to contact us' above).