PRIVACY POLICY

William Sturges LLP takes 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 under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and we are responsible as 'controller' of that personal data for the purposes of the UK GDPR. Our use of your personal data is subject to your instructions, the UK GDPR, the Data Protection Act 2018, other relevant legislation and our professional duty of confidentiality under the SRA Standards and Regulations. We are authorised and regulated by the Solicitors Regulation Authority (SRA).

KEY TERMS

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

We, us, our	William Sturges LLP
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 Data concerning health, sex life or sexual orientation, and genetic and biometric data (where used to identify an individual)
Criminal offence data	Personal data relating to criminal convictions and offences or related security measures

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	Your National Insurance and tax details

Personal data we will collect	**Personal data we may collect depending on why you have instructed us**
Information to enable us to check and verify your identity, e.g. your date of birth, passport details and proof of address	Your bank and/or building society details Details of your professional online presence, e.g. LinkedIn profile
Electronic contact details, e.g. your email address and mobile phone number	Details of your spouse/partner and dependents or other family members, e.g. if you instruct us on a family matter or a will
Information relating to the matter in which you are seeking our advice or representation	Your employment status and details including salary and benefits, e.g. if you instruct us on matter related to your employment or in which your employment status or income is relevant
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	Details of your pension arrangements, e.g. if you instruct us on a pension matter or 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 matter 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 a discrimination claim or your matter is funded by a trade union
	Personal identifying information, such as your eye colour or your parents' names, e.g. if you instruct us to incorporate a company for you

Personal data we will collect	Personal data we may collect depending on why you have instructed us
	Your medical records, e.g. if we are acting for you in a personal injury or medical negligence claim

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, direct. However, we may also collect information:

- from publicly accessible sources, e.g. Companies House 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, 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;
- via our website - we use cookies on our website (for more information on cookies, please see www.allaboutcookies.org and our cookies policy)
- 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 and instant messaging system.

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

What we use your personal data for	Our reasons
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 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 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, including sending publications, updates on the law and details of seminars and other events 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

What we use your personal data for	Our reasons
External audits and quality checks, e.g. for LawNet and ISO 9001 accreditation and the audit of our accounts	For our legitimate interests or 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

We will only process special category personal data, or personal data relating to criminal convictions and offences, where we have both a lawful reason set out above and an additional condition under data protection law applies, for example where:

- you have given your explicit consent;
- it is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- it is necessary for the establishment, exercise or defence of legal claims or for the purpose of obtaining legal advice; or
- it is necessary for reasons of substantial public interest under Schedule 1 of the Data Protection Act 2018, e.g. preventing or detecting unlawful acts or complying with regulatory requirements, including anti-money laundering 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 and details of seminars and other events.

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, for example for certain electronic marketing under the Privacy and Electronic Communications Regulations 2003, 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 sending us an email to law@williamsturges.co.uk or writing to us at Burwood House, 14-16 Caxton Street, London SW1H 0QY.

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;
- our insurers and brokers;
- external auditors, e.g. in relation to LawNet or ISO 9001 accreditation and the audit of our accounts;
- our bank;
- external service suppliers, representatives and agents that we use to make our business more efficient, e.g. typing services, photocopying services, telephone answering services, couriers, case management system providers, website service providers, document collation or analysis suppliers, shredding service providers;
- office cleaners – although we do not share personal data with our office cleaners they do come into our offices to carry out cleaning services and therefore may see personal data.

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.

We may also need to share some personal data with other parties, such as potential buyers of some or all of our business or during 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.

WHERE YOUR PERSONAL DATA IS HELD

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

Some of these third parties may be based outside the United Kingdom. For more information, including on how we safeguard your personal data when this occurs, see below: '**Transferring your personal data out of the United Kingdom**'.

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 and our insurers.

We will not retain your personal data for longer than necessary for the purposes set out in this policy. Different retention periods apply to different types of personal data and are set out in our data retention schedule; however, client files will normally be retained for a minimum of 7 years from the conclusion of the matter, and records obtained for anti-money laundering purposes will be retained for at least 5 years from the end of the business relationship, as required by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

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

TRANSFERRING YOUR PERSONAL DATA OUT OF THE UNITED KINGDOM

To deliver services to you, it is sometimes necessary for us to share your personal data outside the United Kingdom, e.g.:

- with your and our service providers located outside the United Kingdom;
- if you are based outside the United Kingdom;
- where there is a European and/or international dimension to the matter in which we are advising you.

Under data protection law, we can only transfer your personal data to a country or international organisation outside the United Kingdom where:

- the United Kingdom government has decided the particular country or international organisation ensures an adequate level of protection of personal data (known as an "adequacy decision");
- there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for data subjects; or
- a specific exception applies under data protection law.

These are explained below.

Adequacy decision
We may transfer your personal data to certain countries, on the basis of an adequacy decision. These include:

- all European Union countries, plus Iceland, Liechtenstein and Norway (collectively known as the 'EEA');
- Gibraltar; and
- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, Uruguay and the United States (organisations certified under the UK Extension to the EU-US Data Privacy Framework).

The list of countries that benefit from adequacy decisions will change from time to time. We will always seek to rely on an adequacy decision, where one exists.

Other countries or international organisations we are likely to transfer personal data to do not have the benefit of an adequacy decision. This does not necessarily mean they provide poor protection for personal data, but we must look at alternative grounds for transferring the personal data, such as ensuring appropriate safeguards are in place or relying on an exception, as explained below.

Transfers with appropriate safeguards
Where there is no adequacy decision, we may transfer your personal data to another country or international organisation if we are satisfied the transfer complies with data protection law, appropriate safeguards are in place, and enforceable rights and effective legal remedies are available for data subjects.

The safeguards will usually include using the International Data Transfer Agreement or the International Data Transfer Addendum to the EU standard contractual clauses approved under UK data protection law, supported by a transfer risk assessment.

Transfers under an exception
In the absence of an adequacy decision or appropriate safeguards, we may transfer personal data to a third country or international organisation where an exception applies under data protection law, e.g.:

- you have explicitly consented to the proposed transfer after having been informed of the possible risks;
- the transfer is necessary for the performance of a contract between us or to take pre-contract measures at your request;
- the transfer is necessary for a contract in your interests, between us and another person; or

- the transfer is necessary to establish, exercise or defend legal claims

We may also transfer information for the purpose of our compelling legitimate interests, so long as those interests are not overridden by your interests, rights and freedoms. Specific conditions apply to such transfers and we will provide relevant information if and when we seek to transfer your personal data on this ground.

Further information
If you would like further information about data transferred outside the United Kingdom, please contact us (see 'How to contact us' below).

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, e.g. where it is no longer necessary for the purposes for which it was collected, subject to our legal and regulatory obligations to retain it
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; - in certain other situations to our continued processing of your personal data, e.g. processing not necessarily carried out for the purpose of our legitimate interests.
Automated decision-making	The right not to be subject to a decision based solely on automated processing (including profiling) that produces legal or similarly significant effects concerning you. We do not carry out such decision-making.
Withdraw consent	Where we rely on your consent, the right to withdraw that consent at any time, without affecting the lawfulness of processing carried out before withdrawal

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 individuals' rights under the UK General Data Protection Regulation.

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

- email, call or write to us - 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)*;
- where we need it to confirm your identity, let us have proof of your identity and address (e.g. 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.

We will respond to your request within one month of receipt. Where a request is complex or numerous, we may extend this by up to two further months and will tell you why.

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.

HOW TO COMPLAIN

We hope that we can resolve any query or concern you may raise about our use of your information. Please contact our Data Protection Manager in the first instance (see '**How to contact us**' below). Any complaint about our use of your personal data will be recorded, investigated and responded to in accordance with our Complaints Procedure, a copy of which is available on request and on our website.

You also have the right to lodge a complaint with the Information Commissioner, the UK supervisory authority for data protection, who may be contacted at https://ico.org.uk/make-a-complaint or telephone: *0303 123 1113*. If you are dissatisfied with our legal services more generally, you may be able to complain to the Legal Ombudsman once our complaints procedure has been exhausted.

CHANGES TO THIS PRIVACY POLICY

This privacy policy was last updated on 4 November 2026.

We may change this privacy policy from time to time. When we do, we will publish the updated version on our website and, where the changes are significant, notify you directly. This policy is reviewed at least annually, and the current version is controlled under our quality management system.

HOW TO CONTACT US

Please contact us 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	
Tom Walshe, Data Protection Manager tom.walshe@williamsturges.co.uk or Grant Meyrick, Deputy Data Protection Manager grant.meyrick@williamsturges.co.uk	William Sturges LLP Burwood House 14-16 Caxton Street London SW1H 0QY 020 7873 1000