

Bishop & Light SOLICITORS

PRIVACY POLICY & NOTICE

This Privacy Policy and Notice describes how we obtain and use personal data, why we are allowed to do so by law, who has access to personal data and what the rights are of people whose data we hold ("Data Subject"). All Clients of the firm are Data Subjects.

Bishop and Light Solicitors is a firm of Solicitors operating from 5 addresses in Sussex and is committed to protecting and respecting the privacy of Data Subjects.

For the purposes of the Data Protection Act 1998 and the General Data Protection Regulation ("GDPR") the data controller is Bishop and Light Solicitors (Registration Number: Z7561804).

Bishop and Light Solicitors is a firm regulated by the Solicitors Regulation Authority – No. 486954

Bishop and Light has appointed a Data Protection Officer. The identity of the DPO is contained within our Quality Procedures Manual. It may change from time to time. To request the identity of the DPO then e mail law@bishopandlight.co.uk

This Policy and Notice will not routinely be sent to Data Subjects but a summary of the important Privacy issues will be contained in our Terms of Business Letters. These are sent to clients in every case. That letter informs the client that they can request a copy of our Privacy Policy and Notice, should they wish. This Policy and Notice will also be accessible from the home page of our Website at www.bishopandlight.co.uk. In some circumstances we may decide to send the Privacy Notice to a client and this includes, but is not limited to:

- A specific request from the client
- A suspected data breach in respect of that client's personal information
- In circumstances where the Terms of Business letter is not sent.

The following is a broad description of the way this organisation/data controller processes personal information.

Reasons/purposes for processing information

We process personal information:-

1. to provide legal services to our clients
2. to support and manage our employees
3. to support and manage our business

Type/classes of information processed

We process information for the above purposes. This information may include:

- personal details
- family details
- lifestyle and social circumstances
- financial details of
- education and employment details

We also, but only so far as is necessary, process sensitive classes of information that may include:

- physical or mental health details
- racial or ethnic origin
- religious or other beliefs
- political opinions
- sexual life
- offences and alleged offences
- criminal proceedings, outcomes and sentences

Who the information is processed about

We process personal information about:

- clients
- suppliers and service providers
- complainants
- enquirers
- barristers
- advisers, consultants and professional experts
- employees

Who the information may be shared with

Under our Code of Conduct there are very strict rules about who we can share your information with and this will normally be limited to other people who will assist with your matter but may include those that assist us manage our practice and those who regulate us.

This may include:

- Barristers
- medical experts
- courts and tribunals
- collection agencies if you do not pay our bills. healthcare professionals, social and welfare organisations
- business associates
- trade associations and professional bodies
- suppliers and service providers

- ombudsman and regulatory authorities
- training agencies
- complainants and enquirers
- financial organisations
- private investigators
- central government agencies such as the Legal Aid Agency

Where you authorise us we may also disclose your information to your family, associates or representatives and we may also disclose your information in appropriate circumstances to the following:

The EU General Data Protection Regulation (GDPR)

We shall endeavour to ensure that processing of your data by us will be lawful under the GDPR if and to the extent one of the following applies:

- Processing is necessary for the performance of a contract, express or implied, entered into between you and us or to take steps to enter into a contract – Article 6(1)(b);
- Processing is necessary for compliance with a legal obligation – Article 6(1)(c);
- Processing is necessary to protect your vital interests or those of another person – Article 6(1)(d);
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us – Article 6(1)(e);
- Processing is necessary for the purposes of legitimate interests pursued by us or a third party, except where such interests are overridden by your interests, rights or freedoms – Article 6(1)(f).

If you withdraw your consent we may still process your data if that processing falls into one or more of the above categories set out above. If you object to processing performed under Article 6(1)(e) or 6(1)(f), we will stop processing your personal data unless we either:

- Demonstrate a compelling legitimate ground for processing the personal data that overrides the data subject's interests.
- Need to process the personal data to establish, exercise, or defend legal claims.

Where we store personal data

Personal Data is stored in one or more of 4 places:

1. Our Cases management System (Leap) which is Cloud Hosted on secure servers within the UK.
2. We use Microsoft 365 Online where documents, emails and diary entries may contain personal data. This is held on secure Microsoft Servers within the UK.
3. Client files started before 1st January 2015 might be kept in paper form but will be destroyed 6 years from the date of conclusion of the case.
4. Our in house server contains data from our previous Case Management System (ilaw). This data is encrypted, can only be accessed securely using our software. The data has migrated to Leap but is required for management purposes in the short term. It will be erased once no longer needed, estimated as December 2020.

How long we will keep case information - clients

After each matter is completed the file must usually be kept for at least 6 years for Professional Insurance, LAA Audit and SRA requirements. After that date, unless there is a specific reason to keep it longer, it will be destroyed unless we receive written instructions not so to do.

Paper files

Paper files that were started before 1st January 2015 will be destroyed 6 years after the conclusion of the case. The files are stored with our storage Company, Restore PLC, who have signed a confidentiality agreement. There is an established procedure whereby the Accounts Manager regularly reviews which files have exceeded the 6 year time limit and will then arrange destruction of those files.

If a Client wants their file provided to them or destroyed before 6 years then this can be done by Restore PLC sending us the file which can be provided to the client or destroyed.

Digital files

From 1st January 2015 all new files are digital only on the ilaw Case Management System. (CMS)

The CMS has the ability to delete permanently any data stored upon it.

From 1st January 2021 we shall have a system to delete permanently data from the CMS for files on the 6th anniversary of the file being closed. This will delete all data relating to that file. If data on it relates to a client who also has a later matter with the firm then it will not be deleted until the latter file has been closed 6 years.

If before the 6th year anniversary of the conclusion of a digital file we are asked by a client to delete the file and data then subject to exceptions set out above then this can be done.

How long we will keep personal information - others

For employees information shall be retained for 6 years after their employment ends, to ensure compliance with tax legislation, and then destroyed.

Other information will be deleted as soon as it is no longer needed.

Confidentiality

Solicitors are under a professional and legal obligation to keep the affairs of the client confidential. Whilst we will maintain strict confidentiality regarding a client's work generally, we are subject to a number of legal and regulatory requirements and may be required, from time to time, to disclose information to certain authorities for regulatory or taxation reasons.

In particular, the Legal Aid Agency and HM Revenue and Customs have power to inspect our books, records, or client files. Where you are a client it may be necessary for us to instruct

third parties, e.g. accountants, experts, or to communicate with organisations such as the Courts or other official agencies on your behalf and to disclose information about you, including your address and contact details, and facts relating to your matter to enable us and the third party to deal with your instructions as a client and to contact you direct if necessary. We will only do so for the proper conduct of your case.

Children

Where we represent children, their age is verified by the charge document. We see no additional need to verify this.

We do not consider it appropriate to seek parental consent for data processing because in client confidentiality will over-ride the parental rights.

Rights of those whose data we hold

Rights	What does this mean?
1. Rights to be informed	You have the right to be provided with clear, transparent and easily understandable information about how we use your personal data and your rights. This is why we are providing you with the information in this Privacy Policy.
2. Right of access	You have the right to obtain access to your personal data (if we are processing it) and certain other information (similar to that provided in this Privacy Policy). This is so you are aware and can check that we are using your personal data in accordance with data protection law.
3. Right to rectification	You are entitled to have your personal data corrected if it is inaccurate or incomplete.
4. Right to erasure	This is also known as 'the right to be forgotten' and, in simple terms, enable you to request the deletion or removal of your personal data where there is no compelling reason for us to keep using it. This is not a general right to erasure; there are exceptions.
5. Right to restrict processing	You have the right to 'block' or suppress further use of your personal data in certain circumstances. When processing is restricted, we can still store your personal data, but may not use it further.
6. Right of data portability	You have the right to obtain and reuse your personal data in a structured, commonly used and machine-readable format in certain circumstances. In addition, where certain conditions apply, you have the right to have such information transferred directly to a third party.
7. Right to object to processing	You have the right to object to us processing your personal data for our legitimate business interests or for direct marketing purposes (including in each case any related profiling).
8. Right to withdraw consent to processing	If you have given your consent to us to process your personal data for a particular purpose (for example, direct marketing), you have the right to withdraw your consent at any time (although if you do so, it does not mean that any processing of your personal data up to that point is unlawful).

9. Right to make a complaint to the data protection authorities

You have the right to make a complaint to the Information Commissioner's Office (ICO) if you are unhappy with how we have handled your personal data or believe our processing of your personal data does not comply with data protection law.

Access to Information

The Act gives those whose personal data we hold the right to access information held about them. Their right of access is regulated by the Act. Contact details are set out below. Unless it falls within an exception, we shall provide the information within 30 days without charge.

The Data Protection Officer will handle any Subject Access requests. The information will be provided on memory stick, DVD or paper, whichever method is preferred by the Data Subject.

How to contact us

If you would like to exercise your data protection rights or if you are unhappy with how we have handled your personal data, please feel free to contact us by e mail to law@bishopandight.co.uk , by telephone or by letter by post or by hand to any of our addresses:-

Brighton office 171 Edward Street, Brighton, BN2 0JB **Tel** 01273 626288

Hove office Cambridge House, Cambridge Grove, Hove, BN3 3ED **Tel** 01273 732733

Eastbourne office 5 Hyde Gardens, Eastbourne, BN21 4PN **Tel** 01323 434822

Hastings office 66 Bohemia Road, St Leonards on Sea, TN37 6RQ **Tel** 01424 793015

Worthing office Global House, Portland Square, Worthing, BN11 1QH **Tel** 01903 259909

If you are not satisfied with our response to any enquiries or complaint or believe our processing of your personal data does not comply with data protection law, you can make a complaint to the **Information Commissioner's Office (ICO)** by:

- writing to: Information Commissioner's Officer, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF;
- calling: 0303 123 1113; or
- submitting a message through the ICO's website at: ico.org.uk

Data Breaches

We have an established breach report procedure. Any data breach is to be notified via a breach report to the DPO, copying in the Compliance Officer for Legal Affairs (COLP).

Employees must raise a Breach Notification whenever they have reasonable grounds to suspect a Data Breach and send this by e mail to the DPO.

We must notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also have to notify those concerned directly in most cases.

We shall also have to consider whether to inform the SRA of the Breach of SRA regulations.

Data Protection by Design and Data Protection Impact Assessments

We shall endeavour when designing processes to put Data Protection at the forefront of design.

Where appropriate we shall carry out a Data Protection Impact Assessment.

We shall do this in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed;
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

Changes to our Privacy Policy

Any changes we make to our privacy policy in the future will be documented and where appropriate, notified to those whose personal data we hold.