Data Protection and Privacy Policy

Data Protection

The firm is registered with the Office of the Information Commissioner as a Data Controller. This means that we are entitled to hold personal data on clients, staff and others. However, this must be held for a legitimate purpose and the data must be properly protected. We are also bound by the Data Protection Act.

Our professional duties on confidentiality will provide sufficient protection to clients in terms of disclosure of their personal data. However, we are also obliged to ensure that we do not take and hold more data than is necessary and proportionate. You should give consideration to this when taking instructions and requesting data from clients.

The firm holds data on staff that is necessary for the business of the firm and for effective employment, such as details of address, bank account and so on.

It is the policy of the firm to only collect such data as is necessary for the continuation of the firm's business and the provision of services to its clients, to hold that data securely and confidentially, and to hold it only for as long as necessary. Any breach of this policy, such as deliberate or negligent unauthorised release of personal data, will be a disciplinary matter.

Any request by any person for copies of or access to their personal data should be referred to Abuhammad Safiullah.

Our current Data Protection policy is as follows;

Introduction

The purpose of this policy is to enable us to- -

· comply with the law in respect of the data it holds about individuals;

- follow good practice;
- protect our clients, staff and other individuals
- protect the organisation from the consequences of a breach of its responsibilities.

Brief introduction to Data Protection Act 1998

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which make sure that personal information is- -

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the rights of Data Subjects
- Secure
- Not transferred to other countries without adequate protection

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Policy statement

We will -

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently

We recognise that our first priority under the Data Protection Act is to avoid causing harm to individuals. Information about staff and clients will be used fairly, securely and not disclosed to any person unlawfully.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, we will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

We are a Data Controller, registered under the Data Protection Act 1998. All processing of personal data will be undertaken in accordance with the data protection principles.

Definitions

The Data Subject is the individual whose personal data is being processed. Examples include -

- Employees – current and past
- Job applicants
- Users
- Suppliers.

Processing means the use made of personal data including -

- obtaining and retrieving
- Holding and storing
- making available within or outside the organisation
- Printing, sorting, matching, comparing, destroying.

The Data Controller is the legal 'person', or organisation, that decides why and how personal data is to be processed. The data controller is responsible for complying with the Data Protection Act.

The Data Processor - the data controller may get another organisation to be their data processor, in other words to process the data on their behalf. Data processors are not subject to the Data Protection Act. The responsibility of what is processed and how remains with the data controller. There should be a written contract with the data processor who must have appropriate security.

The Data Protection Officer is the name given to the person in organisations who is the central point of contact for all data compliance issues.

Responsibilities

The partnership recognises its overall responsibility for ensuring that we with our legal obligations.

Our registration number with the Information Commissioner's Office is ……

The Data Protection Officer is …… who has the following responsibilities -

- Briefing the partnership on Data Protection responsibilities
- Reviewing Data Protection and related policies
- Advising other staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal data
- Ensuring contracts with Data Processors have appropriate data protection clauses
- Electronic security
- Approving data protection-related statements on publicity materials and letters

Each member of staff who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good Data Protection practice is established and followed.

All staff are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

A staff member noticing a breach of the Data Protection policy must report this to the Data Protection Manager. This applies even if the staff member believes that no harm has been done.

Significant breaches of this policy will be handled under our disciplinary procedures.

Security

This section of the policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspect of security.

Any recorded information will be kept in secure premises, and destroyed confidentially if it is no longer needed. Data must be kept on the computer system only, and must not be copied to personal computers. Staff must keep their computer passwords secure. Staff should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display.

All printed material should be securely shredded when no longer needed. It should not be disposed of in general refuse or non-secure recycling.

Data Recording and storage

We have a single database holding information about all clients. The back-up discs of data are kept in a safe.

We will regularly review our procedures for ensuring that our records remain accurate and consistent and, in particular:

· The database system is reviewed and re-designed, where necessary, to encourage and facilitate the entry of accurate data.

· Data on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets.

· Effective procedures are in place so that all relevant systems are updated when information about any individual changes.

· Data will be corrected if shown to be inaccurate

We store archived paper records in the office or in secure premises provided by storage contractors.

Access to data

In addition to clients' rights as solicitor's clients, all clients have the right to request access to all information stored about them. Any subject access requests will be handled by the Data Protection Officer within the required time limit.

Subject access requests must be in writing. All staff are required to pass on anything which might be a subject access request to the Data Protection Officer without delay.

All those making a subject access request will be asked to identify any other individuals who may also hold information about them, so that this data can be retrieved.

Where the individual making a subject access request is not personally known to the Data Protection Officer their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person.

We will provide details of information to clients who request it unless the information may cause harm to another person.

Staff have the right to access their file to ensure that information is being used fairly. If information held is inaccurate, the individual must notify their supervisor or the Senior Partner, so that this can be recorded on file.

Transparency

We are committed to ensuring that in principle Data Subjects are aware that their data is being processed and

· For what purpose it is being processed;

· What types of disclosure are likely; and

· How to exercise their rights in relation to the data.

Data Subjects will generally be informed in the following ways:

- Staff: in the staff terms and conditions

- Clients: when they request (on paper, on line or by phone) services

Standard statements will be provided to staff for use on forms where data is collected.

Whenever data is collected, the number of mandatory fields will be kept to a minimum and Data Subjects will be informed which fields are mandatory and why.

Consent

Consent will normally not be sought for most processing of information about staff, although staff details will only be disclosed for purposes unrelated to their work for us (e.g. financial references) with their consent.

Information about clients will only be made public with their consent. (This includes photographs.)

'Sensitive' data about clients (including health information) will be held only with the knowledge and consent of the individual.

Consent can be reasonably implied from the retainer with the client.

All Data Subjects will be given the opportunity to opt out of their data being used in particular ways, such as the right to opt out of direct marketing (see below).

Once given, consent can be withdrawn, but not retrospectively. There may be occasions where we have no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

Direct marketing

We will treat the following unsolicited direct communication with individuals as marketing -

- promoting our services

- promoting our events

- Marketing on behalf of any other external company or voluntary organisation

Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all our marketing. We do not have a policy of sharing lists, obtaining external lists or carrying out joint or reciprocal mailings.

We will only carry out telephone marketing where consent has been given in advance, or the number being called has been checked against the Telephone Preference Service.

Whenever e-mail addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

Staff training and acceptance of responsibilities

All staff who have access to any kind of personal data will be given copies of all relevant policies and procedures during their induction process, including the Data Protection policy and the operational procedures for handling personal data.

All staff will be expected to adhere to all these policies and procedures.

We will provide opportunities for staff to explore Data Protection issues through training, team meetings, and supervisions.

Policy review

The policy will be reviewed annually by the Data Protection Officer. It will also be reviewed in response to changes in relevant legislation, contractual arrangements, good practice or in response to an identified failing in its effectiveness.

Privacy policy

Bluestone Solicitors are committed to compliance with relevant UK and European data protection laws and will responsibly protect the information you provide to us and the information we collect in the course of operating our business.

This Privacy Policy describes how Bluestone Solicitors, as data controllers, may collect, use, and share information about you and your rights in relation to that information. Your provision of information to us constitutes your acceptance of the terms of this Privacy Policy. Please do not send us any information about you which you do not want to be used in the ways described in this Privacy Policy.

Scope of this Privacy Policy

This Privacy Policy applies to:

- Your use of our services, including when you request information from us and when you engage Bluestone Solicitors for the provision of legal services.
- Third parties instructed in connection with our provision of legal services to you
- Contractors and suppliers with whom we contract for the purposes of managing and running our business.

Data controller

When we use personal information about you or others in connection with providing our legal services to clients we do so as a data controller.

This Privacy Policy describes:

- The types of information we process
- How we use the information
- How long we retain information
- How we share the information
- Protection and storage of the information
- You and your rights
- How to contact us

The types of information we process

We will process personal information we receive directly from you, on your behalf, other organisations with whom you have dealings, government agencies, publicly available records and the third parties described in 'How we share the information' below.

We may collect current and historical personal information including/relating to: your name, contact details, identification, ethnic origin, marital status, employment/business, finances, academic history and criminal offences/convictions (this is non-exhaustive which depends on the circumstances).

As some personal information is sensitive, we shall seek your consent to process this information. You may withdraw consent at any time as described in 'You and your rights' below.

Debit and Credit Card Information

Receipts of funds in settlement of bills or on account of costs can be processed through …….. We may collect your data to process a credit/debit card transaction, which may be passed onto a third party service provider to complete the financial transaction. Card details will only be held to complete the single transaction. We will not store your card details in our office, physically or electronically. If you use your credit or debit card to make a payment we will ensure this is carried out securely and in accordance with the Payment Card Industry Data Security Standard (PCI-DSS).

How we use the information

Your data will only be used for the service you have requested.

We may use your personal information if:

- It is necessary for the performance of a contract with you or our client on your behalf (e.g. when we are providing our services to you as envisaged by our engagement letter);
- It is necessary in connection with a legal obligation (e.g. when we are carrying out anti-money laundering and conflict checks);
- You have provided your consent to such use (e.g. you have approved the use of a specific third party to assist on your matter);
- We consider such use of your information as not detrimental to you, within your reasonable expectations, having a minimal impact on your privacy, and necessary to fulfil our legitimate interests (e.g. to attend court hearings to represent you, make appointments on your behalf, to manage fees and invoicing, or to recover money owed to us); or
- We are otherwise required or authorised by law.

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
Provide legal services	Your personal data and electronic material that you provide to us which we generating in connection with the legal service that forms the subject of our contract with you	1. You have provided consent 2. It is necessary for the fulfilment of the contract for legal services
If you apply for a job with us	Identity data and contact data, as listed in the application form.	1. Necessary for our legitimate interests (to assess your application and ensure we are properly informed when we interview you) 2. Performance of a contract with you (if you are successful in your application)
Conducting business with you	Identity data (such as name, email address and telephone number).	1. Performance of a contract with you. 2. Necessary for our legitimate interests (particularly maintaining the value of the network referred to above)

Purpose/Activity	Type of data	Lawful basis for processing including basis of legitimate interest
To manage our relationship with you which will include: 1. Notifying you about changes to our terms or privacy policy 2. Asking you to leave a review or take a survey	1. Identity 2. Contact 3. Profile 4. Marketing and Communications	1. Performance of a contract with you. 2. Necessary to comply with a legal obligation. 3. Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)

We also use your information to:

- fulfil our legal requirements (including in relation to anti-money laundering) and professional obligations;
- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

How long we retain information

We recognise that it is important to only retain your personal information for as long as is required by law (which is currently 6 years) or we consider reasonably necessary, after which we will confidentially destroy it.

Records in Immigration Matters

Due to the nature of immigration services, a full record of information obtained from you, third parties and advice provided by us shall not be retained longer than 15 years unless you request that it be erased.

This is because we consider that it is in your best interests that we retain a full history of data which may be relevant to future matters you instruct us to deal with.

Such data can also be relevant to your immigration position should there be any dispute with the authorities or for us to be able to provide you with a record should you misplace important

immigration documents. If you would like us to rectify or erase your data please refer to the section on 'You and your rights' below.

How we share the information

We may share your information with third parties where

- you have provided consent;
- we are under a legal, regulatory or professional obligation to do so (for example, in order to comply with anti-money laundering requirements);
- it is necessary for the purpose of, or in connection with, legal proceedings, or to exercise or defend legal rights;
-

Protection and storage of the information

We hold information securely in electronic or physical form and prevent any unauthorised access, modification or improper disclosure.

Information relating to client's matters is stored in the following ways:

- Paper files
- In personalised electronic files, bearing their own reference on a password protected integrated computer network
- Secure off-site outsourced paper storage following the conclusion of the matter.
-

Our information security practices are supported by a number of security safeguards, processes and procedures. We store information in access controlled premises or in password protected electronic form. We require our third party IT providers to comply with appropriate information security industry standards. All staff and third party providers with access to confidential information are subject to confidentiality obligations.

You and your rights

Subject to applicable laws, you may have certain rights regarding information that we have collected and that is related to you. We encourage you to contact us to update or correct your information if it changes or if you believe that any information that we have collected about you is inaccurate.

You can also ask us to:

- see what personal information we hold about you,
- to erase your personal information
- You may tell us if you object to our use of your personal information.

You have a right to complain to the Information Commissioner's Office (ICO), but we would prefer you to contact us first. We should be able to resolve any matter quickly and to your satisfaction.

The Information Commissioner's Office (ICO) is contactable through their website at https://ico.org.uk/ or their help line on 0303 123 1113 or 01625 545745.

The address of the ICO is:
Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow Cheshire
SK9 5AF

How to contact us

If you would like to contact us with questions about our privacy practices, please contact our Data Protection Manager, on …….....

If you are a data controller or a data processor

If you are a data controller or a data processor in your own right, and you provide personal data to us, you confirm to us that you have a lawful basis for doing so under data protection law and all necessary consents, where required.

Changes to this privacy policy

This is a living document which we may update from time to time.

The Privacy Policy was last reviewed on