Bannister & Co - Solicitors
Privacy Statement

Bannister & Co solicitors are a firm of solicitors who provide legal services and specialise in practising criminal and motoring law. We are regulated by the Solicitors Regulation Authority (SRA) and have a duty to keep information about clients confidential. However, if we are representing clients in court, any information that is given about the client becomes public. For instance, Clients will be asked in open court to confirm their Name, Address, Date of birth and Nationality. The prosecutor will read out in open court details of the prosecution allegations against the client, and we will explain the client's defence and/or mitigation in response. The case may be referred to a Probation officer who may give either a written or oral report to the court and the magistrates will announce in open court their decision about guilt or innocence and if necessary any penalty that they impose upon the client. The magistrates have a duty to explain their reasons in open court. All of this information can be reported by the press.

In May 2018, new regulations came into force which imposes further controls and requirements upon firms or organisations that hold personal information. We are a "controller" under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. **Bannister & Co are registered with Information Commissioners Office (ICO) under registration reference Z4964441**

Whose personal information do we hold?
We may hold personal information about the following people:-
Clients, potential clients and those we have been authorised to communicate with
Co-defendants, witnesses and individuals an investigative authority have told us about
Complainants
Employees
Legal professionals
Suppliers and service providers
Advisers, consultants and other professional experts

What information will we collect?
Clients
We will only collect information from clients that is relevant to the matter with which we are dealing. In particular, we may collect the following information from clients which is defined as "personal data" such as:-
Personal details
Family, lifestyle and social circumstances
Financial details
Business activities

Special Categories - clients
We may also collect information that is referred to as being in a "special category". This could include Physical or mental health details, Racial or ethnic origin, Religious beliefs or other beliefs of a similar nature, Sexual orientation and/or Criminal cautions or convictions

Employees & Service Providers

We will only collect information from Employees that is relevant to the performance of the contract between us. In particular, we may collect the following information from Employees and Service providers which is defined as "personal data" such as:-
Personal details – Name, address, Date of birth
Financial details for banking and payment of salary
Business activities in case it may impact on tax payable by us on your behalf

We will not collect details of Family, lifestyle and social circumstances

Special Categories - Employees
We may also collect information that is referred to as being in a "special category". This could include Physical or mental health details, Racial or ethnic origin, Religious beliefs or other beliefs of a similar nature, Sexual orientation and/or Criminal cautions or convictions. This information will only be collected if it is likely to impact upon your performance at work for the purpose of deciding whether reasonable adjustments will need to be made. Criminal convictions or cautions must be reported to us as they could affect whether we are allowed to employ you on government contracts such as Legal aid.

Processing Activities
Access to the information we hold about clients and service providers is restricted to lawyers and clerical staff who need access to the personal details of clients for the purpose of representation, advice or reporting letters. This information is recorded on the clients file and the firms case management system.

Access to the information we hold on Employees is restricted to the partners and office manager for the purpose of monitoring and performing the contract between us and the payment of salaries. Records are kept of the processing of this information.

Lawful Basis for processing
The Lawful basis on which we process your personal information is one or more of the following:-
Clients and associated persons

1. It is necessary for the performance of our contract with you or to take steps to enter into a contract with a client or associated person
2. It is necessary to deliver our services either under the terms of our Legal Aid Contract or under a private client agreement.
3. It is necessary to comply with a legal obligation either under the terms of our Legal Aid Contract or under a private client agreement.

Clients, employees or service providers

4. It is in our legitimate interest to do so. Examples of Legitimate interest include
    a. Where the data subject is a client or employee or service provider of ours as the controller
    b. Sharing with certain groups for internal administrative purposes
    c. Processing necessary to ensure network and information security, including preventing unauthorised access
    d. Processing for the prevention of fraud, or in accordance with our reporting responsibilities under Money Laundering regulations, criminal acts and threats to public security

Clients, employees or service providers

5. Consent this can be withdrawn at any time by advising our data protection manager but does not affect the fact that we will continue to hold your personal details for any or all of the other categories.

How will we use Personal information?
We may use personal information for the following purposes:-
Provision of legal services including advising and acting on behalf of our clients
Maintaining accounts and records
Business administration and legal compliance
Proper performance of a contract of employment
Provision of education and training to our employees
Supporting and managing employees

Who will we share personal information with?
As Solicitors we are bound by rules of confidentiality. There are very strict rules about who we can share client information with and where permitted this will normally be limited to other people who will have dealings with the client's matter. This may include:-
Our solicitor or police station agents
The Court and court staff
Prosecuting agencies and the police
Co-defendants and their lawyers
Court appointed experts including medical experts
Experts
Barristers and their clerks
Healthcare professionals
The National Probation Service
Professional bodies and other outside auditors and assessors including the Solicitors Regulation Authority, the Legal Aid Agency, our Lexcel Auditors and the Legal ombudsman Accountants
If a client authorises us we may also disclose personal information to a client's family, associates or representatives.

When instructing barristers or experts on behalf of a client we will ensure that they also have a privacy policy under the General Data Protection Regulations and if not we will either instruct different barristers or expert or ask them to enter into a Data sharing agreement with requirements for them to retain the information that we share securely and confidentially.

We will not supply personal data to other organisations for the purpose of marketing.

Data Protection Training
The Data Protection Manager will review this policy every 6 months and at the same time will provide training for all staff as a reminder of the importance of Data protection

Review of Processing operations
The GDPR regulations require Data Controllers to have Data Protection by design and default. Bannister and Co solicitors have been managing personal data of employees and Clients for over 20 years. The greater use of computers and e mails has increased the risk of data loss by either hackers, virus, or mismanagement of e mails. All computers are encrypted and have virus protection which is automatically updated on a daily basis. The off-site back up is encrypted. The Data Protection Manager has

recorded all data processing activities and carried out a Data Protection Impact Assessment in relation to recruitment processes and clients. This will be reviewed every 6 months and in the event of any data loss.

The Data Protection Manager will carry out a Data Protection Impact Assessment whenever there is a change to the information that we collect and/or how we collect it. The Data Protection Manager will consider the following screening questions:-

These questions are intended to help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. The answers can be expanded as the project develops if necessary.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Will the project have any risk to the security of the data that we hold, either through loss or the transmission of it?

How long will we keep this information for?
We will normally keep information throughout the period of time that we do work for Data Subjects or an employee is employed by us. This information will be retained for a period of at least six years as we are required to do so by law and also by our contract with the Legal Aid Agency and regulations that apply to us. In particular, the Legal aid Agency can require us to produce a copy of the original on line submission declaration form signed when applying for legal aid. This requirement can be at any time during or after the Contract period but no later than six years from the date the contract ends. Our current contract with the LAA expires in 2022, but could be extended by them. Data retention timescales will be reviewed every 6 months when this policy is reviewed

Transfer to third countries

We do not envisage any transfer of personal information to a country outside the EEA. We do not use cloud computing, if we do need to transfer for any reason we will ensure that appropriate safeguards are in place at all times.

Security arrangements
We shall ensure that all the information that we hold is kept secure using appropriate technical and organisational measures

We are accredited under Lexcel and have security measures in place

In the event of a personal data breach we will take steps to ensure that effects of such a breach are minimised and shall liaise with the ICO and with the subject of the data breach as appropriate.

The first step where there is a data breach is for the partners to be notified. They will take immediate steps to identify whether the breach relates to one or more data subjects, and identify how the breach happened. If the data breach has been caused by a disclosure by an employee either deliberately or inadvertently, then the partners will decide how to minimise the risk of the data breach being further disclosed. For example if a client's data has been disclosed to another client inadvertently by sending an e mail to the wrong address, then the recipient of the data will be contacted and they will be asked to meet with a partner who will supervise the deletion of the information. The client will be notified of the disclosure and the action being taken. The partners will decide whether it is necessary to make a report to the ICO.

If there has been a personal data breach, the Data Protection Manager will consider whether this poses a risk to people, and the likelihood and severity of any risk to people's rights and freedoms, following the breach. If it is likely there will be a risk then the ICO must be notified. If it is unlikely to pose a risk to people then it does not have to be reported. **It is not necessary to report every breach to the ICO.**

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When deciding about a personal data breach and when we need to report it, we will consider the advice given by the ICO on the personal data breach pages of the ICO's our Guide to the GDPR.

What rights do Data Subjects have?
Data Subjects have the following rights under GDPR:-
Right to be informed
Right of access
Right to rectification
Right to erasure
Right to restriction of processing
Right to data portability

Right to object
Rights concerning automatic decision-making and profiling

Right of access
Data Subjects have a right to see the information that we hold about them
To access this Data Subjects should be asked to provide a request in writing to our data protection officer together with proof of identity. All requests will immediately be forwarded to the Data protection manager who will usually process requests free of charge and within 30 days but we reserve the right to charge a reasonable administrative fee. In some circumstance, it may be necessary to extend the period of time by a further two months if the request is very complex

Right to erasure
Data subjects have a right to ask us to erase their personal information in certain cases (details may be found in Article 17 of the GDPR)
To access this Data Subjects should be asked to provide a request in writing to our data protection manager together with proof of identity. All requests will immediately be forwarded to the Data protection manager who will usually process requests free of charge and within 30 days but we reserve the right to charge a reasonable administrative fee. In some circumstance, it may be necessary to extend the period of time by a further two months if the request is very complex

Data Protection Manager and how to complain
If a data Subject is unhappy about how we are using their information or how we have responded to their request then initially they should be advised to contact our data protection officer,
Jeffrey Bannister,
Bannister and Co - Solicitors
Tudor Chambers
Manor Road
Yeovil
BA20 1UQ

01935 433133

info@bannisterandco.uk

If any complaint remains unresolved then the Data Subject can contact the Information Commissioner's Office, details available at www.ico.org.uk

Changes to this Privacy Statement
We may make changes to this Privacy Policy from time to time. To ensure that Data Subjects are always aware of how we use their personal information we will update this Privacy Statement from time to time to reflect any changes to our use of any personal information. We may also make changes as required to comply with changes in applicable law or regulatory requirements. Where it is practicable, we will notify Data Subjects by email of any significant changes. However, we encourage Data subjects to review this Privacy Statement periodically to be informed of how we use personal information. Our most up to date Privacy statement can be found on our website.

Jeffrey Bannister – 20 May 2018

Reviewed Jeffrey Bannister 14 November 2018