

The Chambers of Ian Jobling takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (“GDPR”) and the Data Protection Act 2018 (“DPA 2018”) together Data Protection Legislation seriously.

The Chambers of Ian Jobling obtains, uses, stores and otherwise processes personal data relating to potential staff, current staff, former staff, current and former workers, contractors, website users and clients, collectively referred to in this policy as data subjects. When processing personal data, the Chambers of Ian Jobling is obliged to fulfil individuals’ reasonable expectations of privacy by complying with the Data Protection Legislation.

This policy therefore seeks to ensure that we:

- i) are clear about how personal data must be processed and the Chambers of Ian Jobling expectations for all those who process personal data on its behalf;
- ii) comply with Data Protection Legislation and with good practice;
- iii) protect the Chambers of Ian Jobling reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects’ rights; and
- iv) protect the Chambers of Ian Jobling from risks of personal data breaches and other breaches of Data Protection Legislation.

This policy applies to all personal data we process regardless of the location where that personal data is stored and regardless of the data subject. All staff and others processing personal data on the Chambers of Ian Jobling behalf must read it. A failure to comply with this policy may result in disciplinary action.

The Chambers of Ian Jobling Data Protection Officer (DPO) is Ian Jobling, he can be reached at ian@ianjobling.com

Personal Data Protection Principles

When you process personal data, you should be guided by the following principles, which are set out in the Data Protection Legislation.

The Chambers of Ian Jobling is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

- i) processed lawfully, fairly and in a transparent manner;
- ii) collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- iii) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- iv) accurate and where necessary kept up to date;
- v) not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed; and
- vi) processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

- i) where the legal basis of our processing is Consent, to withdraw that Consent at any time;
 - ii) to ask for access to the personal data that we hold;
 - iii) to prevent our use of the personal data for direct marketing purposes;
 - iv) to object to our processing of personal data in limited circumstances;
 - v) to ask us to erase personal data without delay;
 - vi) if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed we must cease processing the personal data;
 - vii) to ask us to rectify inaccurate data or to complete incomplete data;
 - viii) to restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
 - ix) to ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
 - x) the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the Chambers of Ian Jobling;
 - xi) to prevent processing that is likely to cause damage or distress to the data subject or anyone else;
 - xii) to be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
 - xiii) to make a complaint to the ICO; and
 - xiv) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format
- .

Who is accountable.

The Chambers of Ian Jobling must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles.

The Chambers of Ian Jobling is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document Data Protection Legislation compliance.

Who is responsible.

As the Data Controller, the Chambers of Ian Jobling is responsible for establishing policies and procedures in order to comply with data protection law.

Where external companies are used to process personal data on behalf of the Chambers of Ian Jobling, responsibility for the security and appropriate use of that data remains with the Chambers of Ian Jobling.

Reporting a breach.

The Data Protection Legislation requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the

risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so. The Data Protection Legislation restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

The Data Protection Legislation requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

We are required to ensure that all staff undergo adequate training to enable them to comply with data protection law.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

The Sharing of Public Data

Some bodies have a statutory power to obtain information. You should seek confirmation of any such power before disclosing personal data in response to a request. Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders.

We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy. This policy was approved on the 2nd September 2025. It will be reviewed in September 2026.