

# DATA PROTECTION POLICY

## Policy Statement

Cloisters and its members[[1]](#footnote-1) are committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 (**DPA**) (collectively **the Data Protection Legislation**).

**Scope**

This Policy applies to data processing carried out by:

* Members of Cloisters (tenants and associate tenants), both in respect of data processing carried out on behalf of Cloisters and in their capacity as Data Controllers in their own right;
* Pupils;
* Employees (permanent and temporary); and
* Agency and contract staff.

The Data Protection Legislationand this Policy apply to all personal data processing functions (on computers or stored in manual (paper based) files), including those performed in relation to the personal data of members (both tenants and associate tenants), as well as pupils and mini-pupils, applicants for tenancy, employment and pupillage, clients, employees and suppliers and any other personal data we process from any source.

Any breach of the Data Protection Legislationand/or this Policy will be dealt with under Cloisters’ Disciplinary Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partner organisations and third parties working with or for Cloisters which have or may have access to personal data processed by or on behalf of Cloisters will be expected to adhere to all obligations imposed by the Data Protection Legislation. No third party may access personal data held by Cloisters without having first entered into a Data Sharing/Processing Agreement which imposes, on that third party, obligations which are no less onerous than those to which we are committed, and which gives Cloisters the right to audit their compliance with data protection requirements.

## Definitions

The Data Protection Legislationapplies to the **processing of personal data** wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

The Data Protection Legislationapplies to all Data Controllers that are established in the European Union (EU) who process the personal data of Data Subjects. It also applies to Data Controllers outside the EU who process personal data in order to offer goods and services to, or monitor the behaviour of, Data Subjects who are resident in the EU.

**Child –** the GDPR defines a child as anyone under the age of 16 years, although the UK may lower this to the age of 13. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. The data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

**Consent -** means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

**Data breach –** a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. The data controller is required to report data breaches to the Information Commissioner’s Office (ICO), particularly breaches likely to adversely affect the personal data or privacy of the Data Subject.

**Data Controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by EU or Member State law.

**Data Subject** – any living individual who is the subject of personal data held by an organisation.

**Personal data** – any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

* **Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a living person, data concerning health or data concerning a living person's sex life or sexual orientation.

**Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Third party** – a natural or legal person, public authority, agency or body other than the Data Subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

## Responsibilities and Roles

Cloisters is a Data Controller within the meaning of the Data Protection Legislation and is registered with the ICO under the names of its Joint Heads of Chambers (Robin Allen QC, ICO registration number Z5968196 & Joel Donovan QC, ICO registration number Z4755875).

Claire McCann is the Data Compliance Lead (**DCL**) and is responsible for monitoring compliance with this Policy, alongside the Head(s) of Chambers and Cloisters’ Management Committee.

The Heads of Chambers, Cloisters’ Management Committee and all those in managerial or supervisory roles throughout chambers are responsible for developing and encouraging good information handling practices within the organisation. Cloisters has an IT & Information Security Management Policy (which can be accessed via its intranet).

Our DCL is directly accountable to the Heads of Chambers for the management of personal data within our organisation and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes ensuring the development and implementation of all necessary processes and procedures, including security and risk management, to ensure compliance with the Data Protection Legislation.

Our DCL is the first point of call for anyone seeking clarification on any aspect of data protection compliance within the organisation and should be informed about any data breach and any Data Subject Access Request (**DSAR**).

Compliance with the Data Protection Legislation is the responsibility of everyone at Cloisters who processes personal data.

Employees are responsible for ensuring that any personal data about them and supplied by them to us is accurate and up-to-date.

Our DCL and/or other individual designated by Cloisters’ Management Committee will ensure that a regular review of data protection compliance is carried out.

## Data Protection Principles

All processing of personal data must be conducted in accordance with the six Data Protection Principles **(“the Principles**”) as set out in the Data Protection Legislationand outlined below. Our policies and procedures are designed to ensure compliance with these Principles.

1. **Personal data must be processed lawfully, fairly, and transparently**

***Lawful*** – Cloisters needs to identify a lawful basis before personal data can be processed.

***Fairly*** – in order for processing to be fair, certain information must be made available to Data Subjects. This applies whether the personal data was obtained directly from Data Subjects or from other sources.

***Transparently*** – the Data Protection Legislationincludes rules on giving privacy information to Data Subjects. These privacy notices are detailed and specific, placing an emphasis on making them understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

1. **Personal data can only be collected for specific, explicit, and legitimate purposes**

The personal data obtained for specified purposes must not be used for a purpose that is incompatible with those formally notified to the ICO as part of the registration of processing carried out by Cloisters and its members.

1. **Personal data must be adequate, relevant, and limited to what is necessary for processing**

Information must not be collected that is not strictly necessary for the purpose for which it is obtained.

1. **Personal data must be accurate and, where necessary, kept up to date.**

Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. Data that is stored must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

1. **Personal data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing.**

Personal data should only be kept for as long as it is needed for the purposes for which it is being processed.

1. **Personal data must be** **processed in a manner that ensures appropriate security of the personal data**

This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

**Demonstrating Accountability**

The Data Protection Legislationincludes provisions that promote Accountability and Governance. These complement the Data Protection Legislation’s transparency requirements. Accountability requires Cloisters to demonstrate compliance with the Data Protection Principles.

Cloisters will demonstrate compliance with the Principles by implementing and adhering to data protection policies and privacy notices, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by Design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

## Data Subjects’ Rights

The Data Protection Legislation provides the following rights for individuals in relation to their personal data:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Data Subjects may make a DSAR relating to their personal data. The Subject Access Request Policy describes how Cloisters will ensure that all responses to DSARs comply with the requirements of the Data Protection Legislation.

Cloisters will normally respond to requests for information from Data Subjects within one calendar month in accordance with the Subject Access Request Policy. This can be extended to two months for complex requests in certain circumstances. If we decide not to comply with the request, we will respond to the Data Subject to explain our reasoning and inform them of their right to complain to the ICO and/or seek a judicial remedy.

Data Subjects have the right to complain to us about the processing of their personal data, the handling of a DSAR and to appeal against how their complaints have been handled.

## 

## Consent

We understand ‘consent’ to mean that it has been explicitly and freely given, and it is a specific, informed and unambiguous indication of the Data Subject’s wish that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Data Subject can withdraw their consent at any time.

We also understand ‘consent’ to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Consent cannot be inferred from non-response to a communication. As Data Controller, we must be able to demonstrate that consent, where necessary, was obtained for the processing operation.

For Sensitive Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists. Cloisters and its Members have set out the lawful bases for their data processing in their Privacy Notices which are published via Cloisters’ website and/or intranet portal.

## Collection of Data

All data collection forms (electronic and paper-based) must include a fair processing statement or a link to our Privacy Notice. For data collection via Cloisters’ website, our Privacy Notice is published on the website.

## Accuracy of Data

We are responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

Staff must notify their manager or Cloisters’ Office Manager of any changes in their personal circumstances which may require personal records to be updated accordingly.

Cloisters will ensure that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Cloisters will also make appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date personal data to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

## Security of Data

All personal data should be accessible only to those who need to use it. All personal data should be treated with the highest security as set out in the IT & Information Security Management Policy.

Cloisters will carry out a regular risk assessment taking into account all the circumstances of the various data processing operations.

In determining the appropriateness of Cloisters’ technical and organisational security measures, consideration will be given to the extent of possible damage or loss that might be caused to individuals (e.g. staff or clients) if a security breach occurs, the effect of any security breach on chambers itself, and any likely reputational damage, including the possible loss of client trust.

It is strictly prohibited to remove personal data from Cloisters’ premises for any reason other than carrying out legitimate processing activities.

Processing of personal data ‘off-site’ presents a potentially greater risk of loss, theft, or damage to personal data and the precautions that must be taken are set out in the IT & Information Security Management Policy.

All staff are responsible for ensuring that any personal data held by Cloisters and for which they are responsible is kept securely and is not, under any condition, disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a Data Sharing/Processing Agreement.

Data breaches and/or incidents will be dealt with in accordance with Cloisters’ internal processes relating to data breaches.

## Disclosure of Data

Personal data must not be disclosed to *unauthorised* third parties, which includes family members, friends, government bodies, and, in certain circumstances, the Police.

All those governed by this Policy must exercise caution when asked to disclose personal data held on another individual to a third party.

All requests to provide personal data to third parties must be supported by appropriate authorisation, given by the DCL and/or the Head(s) of Chambers (or other person designated by Heads of Chambers), or by a relevant Data Sharing/Processing Agreement.

## Retention and Disposal of Data

Cloisters shall not keep personal data in a form that permits identification of Data Subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

The retention period for personal data is set out in our Retention and Disposal Policy.

Personal data will be retained in line with our Retention and Disposal Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

Cloisters will undertake a regular review of the retention dates of all the personal data which it processes and will identify any data that is no longer required. This data will be securely archived, deleted or destroyed in line with the Retention and Disposal Policy.

Where personal data is archived, it will be minimised, encrypted, or pseudonymised, where appropriate and in order to protect the identity of the Data Subject in the event of a data breach.

Our DCL and/or the Head(s) of Chambers must specifically approve any data retention that exceeds the retention periods defined in our Retention and Disposal Policy and must ensure that the justification is clearly identified and recorded.

Cloisters may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject.

## International Data Transfers

Under the Data Protection Legislation, transfers of personal data to third countries outside the European Economic Area (**EEA**) can only be made if specific safeguards exist.

Cloisters does not normally transfer any personal data to a third country outside the EEA and no such transfer shall be permitted until authorisation has been sought from the DCL and/or the Head(s) of Chambers (or other designated person) who have confirmed in writing that appropriate safeguards are in place.

If Cloisters is required to transfer data outside the EEA, we will ensure that we have satisfied ourselves that the conditions laid down in the Data Protection Legislation are complied with by the data controller and/or data processor to whom we transfer that data, by way of:

* + 1. **An adequacy decision, or**
    2. **Privacy Shield, or**
    3. **Binding corporate rules, or**
    4. **Model contract clauses, or**
    5. **Exceptions**
* the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;
* the transfer is necessary for the performance of a contract between the Data Subject and the data controller or the implementation of pre-contractual measures taken at the Data Subject's request;
* the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the data controller and another natural or legal person;
* the transfer is necessary for important reasons of public interest;
* the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
* the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

## Data Protection Impact Assessments (DPIAs)

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of living peoples, we shall, prior to the processing, carry out a Data Protection Impact Assessment of the envisaged processing operations. All DPIAs should be led or overseen by the DCL.

Where, as a result of a DPIA, it is clear that Cloisters is about to commence processing of personal data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not such processing may proceed must be referred to the Management Committee and/or the Head(s) of Chambers for approval to proceed.

Cloisters’ DCL (or other person designated by our Head(s) of Chambers and/or the Management Committee) shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, refer to the ICO for guidance and advice.

**Complaints**

Complaints relating to breaches of the Data Protection Legislation and/or complaints that an individual’s personal data is not being processed in line with the data protection principles should be referred to the DCL and/or the Head(s) of Chambers without delay.

**Penalties**

It is important that members of Cloisters and everybody working for chambers understands the implications if we fail to meet our data protection obligations. Failure to comply could result in:

* Criminal and civil action;
* Fines and damages;
* Personal accountability and liability;
* Suspension / withdrawal of the right to process personal data by the ICO;
* Loss of confidence in the integrity of Cloisters’ systems and procedures;
* Irreparable damage to chambers’ reputation.

**Note: Chambers could be fined up to €20M or up to 4% of the total annual turnover of the preceding financial year, whichever is higher**

1. References to “Cloisters” are to the barristers’ chambers known as Cloisters at 1 Pump Court, Temple, London EC4Y 7AA, which is composed of its Members (tenants and associate tenants) whose membership of Cloisters is governed by its Constitution. [↑](#footnote-ref-1)