Kenneth Elliott & Rowe Limited

Data Protection Policy

Introduction

Kenneth Elliott & Rowe Limited is a law firm and provides legal advice and assistance to its clients. It is regulated by the Solicitors Regulation Authority.

The personal data that the firm processes to provide these services relates to its clients and to other individuals as necessary, including people on the other side of matters, witnesses, beneficiaries, staff and suppliers' staff.

This policy sets out the firm's commitment to ensuring that all personal data it processes, including special category personal data and criminal offence data, is handled in compliance with data protection law. The firm ensures that good data protection practice is embedded in the culture of our staff and our organisation.

Related policies and procedures

- record of processing activities
- privacy notices (website, clients, employees)
- personal data breach reporting process and breach register
- data retention policy
- data subject rights procedure
- data protection impact assessment process
- transfer risk assessment process
- **data protection complaints procedure** (new — required by section 164A of the Data Protection Act 2018)
- **artificial intelligence use policy** (new)
- IT security policies

What we mean by data protection law

In this policy, "data protection law" means the UK General Data Protection Regulation and the Data Protection Act 2018, both as amended by the Data (Use and Access) Act 2025, together with the Privacy and Electronic Communications Regulations 2003 and any other applicable UK data protection legislation.

The main data protection changes made by the Data (Use and Access) Act 2025 took effect on 5 February 2026. The duty to operate a complaints procedure took effect on 19 June 2026.

Scope

This policy applies to all personal data processed by the firm and is part of the firm's approach to compliance with data protection law. All staff are expected to comply with it. Failure to comply may lead to disciplinary action for misconduct, including dismissal.

Obtaining, accessing or disclosing personal data in breach of this policy may also be a criminal offence under section 170 of the Data Protection Act 2018.

Data protection principles

The firm complies with the data protection principles. When processing personal data, it ensures that:

- it is processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)
- it is collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (purpose limitation)
- it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation)
- it is accurate and, where necessary, kept up to date, and that reasonable steps are taken to erase or rectify inaccurate personal data without delay (accuracy)
- it is kept in a form which permits identification of data subjects for no longer than is necessary (storage limitation)
- it is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality)

The firm is responsible for, and must be able to demonstrate compliance with, these principles (accountability). This is why the documentation listed above is maintained and kept current.

How we apply this in practice

The firm will:

- identify the lawful basis for processing personal data in advance and record it, including where it relies on the recognised legitimate interests introduced by the Data (Use and Access) Act 2025
- not do anything with personal data that the data subject would not expect, given this policy and the relevant privacy notice
- ensure that appropriate privacy notices are in place advising clients, staff and others how and why their data is processed, and in particular advising them of their rights
- collect and process only the personal data it needs for purposes identified in advance
- take reasonable steps to keep the personal data it holds accurate and up to date
- retain personal data only for as long as it is needed, in accordance with the data retention policy, and then securely delete or destroy it
- ensure appropriate technical and organisational security measures are in place so that personal data can only be accessed by those who need it, and is held and transferred securely
- carry out a data protection impact assessment before beginning any processing likely to result in a high risk to individuals, including the introduction of new technology
- ensure that all staff who handle personal data are aware of their responsibilities and are adequately trained and supervised

Data subject rights

The firm has processes in place to facilitate requests by individuals to exercise their rights. All staff receive training, can identify such a request, and know who to send it to. Requests must be forwarded to the data protection lead on the day they are received.

Requests are considered without undue delay and within one month of receipt. That period may be extended by up to two further months where the request is complex or where a number of requests have been made, in which case the data subject will be told within the first month.

Subject access

The right to be told whether personal data is being processed, to be given access to that data and a copy of it, and to be given the purposes of the processing, the categories of personal data, the recipients, the retention period, the source of the data if not collected from the data subject, the existence of any automated decision-making, and the right to complain.

Two points confirmed by the Data (Use and Access) Act 2025 apply:

- **Reasonable and proportionate searches.** The firm is required to carry out a reasonable and proportionate search for the personal data requested. It is not required to search exhaustively.
- **Stopping the clock.** Where the firm reasonably requires further information in order to respond, the time limit is paused until that information is received. The firm must be able to demonstrate that the clarification was reasonably required, so the reason must be recorded.

Other rights

Rectification: to have inaccurate personal data corrected.

Erasure: to have data erased, but only where it is no longer necessary for the purpose for which it was collected, consent is withdrawn and there is no other basis, there is no legal basis for the processing, or there is a legal obligation to delete it. The firm will frequently be unable to erase matter file data because of its regulatory and legal retention obligations, and will explain this where it applies.

Restriction of processing: to ask that processing be restricted where accuracy is contested, where processing is unlawful but the data subject does not want erasure, where the firm no longer needs the data but the data subject requires it for legal claims, or pending verification of an objection.

Data portability: to receive a copy of personal data provided by the data subject and processed by automated means, in a transferable format. This applies only where the firm processes on the basis of consent or contract.

Object to processing: to object to processing carried out on the basis of legitimate interests, unless the firm can demonstrate compelling legitimate grounds which override the data subject's interests, or the processing is for the establishment, exercise or defence of legal claims.

The right to complain to the firm

Since 19 June 2026, section 164A of the Data Protection Act 2018 has given data subjects the right to complain to the firm directly about how their personal data has been handled. The firm must acknowledge a complaint within 30 calendar days and take appropriate steps to respond without undue delay.

This right is separate from the right to complain to the Information Commissioner's Office, and separate again from the firm's client complaints procedure, which deals with the quality of legal service and carries a right of referral to the Legal Ombudsman. The Data Protection Complaints Procedure explains how all three fit together.

Special category and criminal offence data

Special category data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, together with genetic data, biometric data used to identify a person, data concerning health, and data concerning a person's sex life or sexual orientation. Data about criminal convictions and offences is subject to separate, similar restrictions.

The firm processes special category and criminal offence data of clients and third parties where necessary to provide legal services, principally in reliance on the condition for the establishment, exercise or defence of legal claims and the condition for the provision of legal advice. It processes special category data of employees where necessary to comply with employment and social security law.

This data attracts additional protection. In particular it must not be entered into any artificial intelligence tool except in accordance with the Artificial Intelligence Use Policy, and it must never be used to make a decision about a person by automated means without meaningful human involvement.

Automated decision-making

Articles 22A to 22D of the UK GDPR replaced the former Article 22 on 5 February 2026.

A decision is a significant decision if it produces legal effects or similarly significant consequences for a data subject, and it is based solely on automated processing if there is no meaningful human involvement in taking it.

- Where a significant decision is based wholly or partly on special category data, it may not be taken solely by automated means unless the data subject has given explicit consent or another narrow statutory justification applies.
- Where no special category data is involved, a significant automated decision is permitted provided the firm gives the data subject information about the decision, allows them to make representations, provides for human intervention, and allows them to contest it.

The firm's position is that no decision affecting a client, an employee or any other individual is taken by automated means. Every output of any automated or AI-assisted process is reviewed by a person who takes responsibility for it. Staff must not adopt an AI output without applying their own judgement to it; a review that is nominal rather than genuine would put the firm inside the automated decision-making regime.

Artificial intelligence

The firm uses approved artificial intelligence tools to assist with legal work. All such use is governed by the Artificial Intelligence Use Policy, which sets out which tools are approved, what information may and may not be entered into them, the verification required before any output is relied on, and the position on client consent.

No personal data may be entered into any AI tool that has not been approved by the firm, and personal AI accounts must never be used for firm work.

International transfers

The firm restricts transfers of personal data outside the United Kingdom. Where a transfer is necessary, it will take place only where the destination is covered by UK adequacy regulations, or where an appropriate safeguard is in place, normally the International Data Transfer Agreement or the UK Addendum to the EU standard contractual clauses.

Where the firm relies on a safeguard it will carry out a transfer risk assessment applying the data protection test introduced by the Data (Use and Access) Act 2025: whether the standard of protection for data subjects in the destination is not materially lower than under UK law. The assessment is made acting reasonably and proportionately, having regard to the nature, volume and sensitivity of the data, and is recorded.

Personal data breaches

Any actual or suspected personal data breach must be reported to the data protection lead immediately on discovery. Staff must not attempt to assess the seriousness of a breach themselves or wait until they have established the facts.

The firm will assess whether the breach is notifiable to the Information Commissioner's Office within 72 hours of becoming aware of it, and whether the individuals affected must be told. All breaches are recorded on the breach register whether or not they are notifiable.

Responsibility for the processing of personal data

The directors of Kenneth Elliott & Rowe Limited take ultimate responsibility for data protection.

If you have any concerns, or wish to exercise any of your rights under data protection law, you can contact the data protection lead:

> **Mark Sadler**
> Kenneth Elliott & Rowe Limited
> Enterprise House, 18 Eastern Road, Romford, Essex RM1 3PJ
> mbs@ker.co.uk
> 01708 757575

Monitoring and review

This policy takes effect on 22 July 2026 and replaces all previous versions.

It will be reviewed at least annually, and additionally whenever there is a material change in the law, in regulatory guidance, or in the firm's processing — including the introduction of any new artificial intelligence tool. The data protection lead is responsible for initiating each review and for recording that it has taken place.

Approved by	The directors of Kenneth Elliott & Rowe Limited
Version	2.0
Effective from	22 July 2026