RETENTION (OF DATA) POLICY

This Retention Policy forms part of Stone Rowe Brewer's overall Data Protection and Information Management and Security Policy as embedded in the Firm's Quality Procedures Manual and it should be read and considered in that context. This Policy has been revised by reference to the GDPR as introduced on 25th May 2018. The Policy has also been reviewed at the AQR 2021 and by the Data Protection Officer in June 2022

General Policy	The Firm's general policy as to retention of data is that data will not be retained beyond the time when it is necessary to do so.
Considerations	Unless a client specifically requests the erasure of data or requests to be forgotten, the following considerations will be taken into account: • Case documents may be relevant to an appeal out of time. • File documents can be used as precedents. • Data on file is specifically retained for legal purposes only • Data and documents are of significant value and benefit to the data subject within subsequent matters, cases and transactions

Considerations (continued)	• Case documents may contain the results of research into the law, which may be relevant to a current case. • Instructions, facts or expert opinions in a previous case may be relevant to a current case. • Correspondence or instructions contain contact details which may be useful. • File documents or records may be important when carrying out a conflict search. • Case documents have to be retained in the event that a complaint is made against a solicitor, or a solicitor makes a claim against his or her insurers. • In the context of a law firm, experience identifies that most clients prefer the retention of their data to provide a smooth transition between one matter and another-for example, clients' Wills or copies of their Wills are stored indefinitely • Periodic review of this policy (including at the Annual Quality Review in September 2021) has established the importance of the retention of sensitive data (including bank account details and e-mail addresses) in order to avoid and/or mitigate the possibility of contributing to fraudulent activity
Storage Policy	The Firm's policy as to storing data securely includes: • In cases when data is stored on printed paper, it should be filed promptly and kept in a secure place where unauthorised personnel cannot access it • Printed data should be shredded when it is no longer needed

Storage Policy (continued)	• Data stored on a computer should be protected by strong passwords • Data is not generally stored on CDs or memory sticks but if it is then they should be locked away securely when they are not being used • The DPO must approve any cloud used to store data • Our servers containing personal data are kept in a secure location, away from general office space • Data should be regularly backed up in line with the Firm's backup procedures • Data should never be saved directly to mobile devices such as laptops, tablets or smartphones • All servers containing sensitive data must be approved and protected by security software and a strong firewall • At the conclusion of files/matters, the Firm's archiving policy is to store information securely on its intranet and in that regard such information and data is encrypted.
Duties as a Law Firm	We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained. As a Law Firm, we have duties to retain data for a period of 6 years and in various types of transactions, such as personal injury or clinical negligence cases involving children or in family or matrimonial matters, the retention period may be longer of necessity. As identified above (Page 2), periodic review of this policy has prompted a change in policy in relation to the retention of bank account and other personal details as an

Duties as a Law Firm (cont.)	essential component in resisting fraudulent activity. Furthermore, pursuant to the latest money laundering regulations, we have a specific duty to retain all data and documentation relating to our compliance with those regulations for a minimum period of 5 years.
Special Category Data	The Firm's policy is that, except in certain circumstances, special category data will be deleted and/or destroyed at the point of archiving the data subject's file or matter after the conclusion of the transaction in question. Examples of the certain circumstances when special category data may be retained for longer are: • In litigation matters where an appeal out of time may be a possibility • In legal matters relating to children where it may be necessary to re-open or re-visit the matter at a later date • In Trust or tax matters • Will retention • Administration of Estates • Family matters where applications, court orders are re-visited/re-opened • When ID documents are retained with the consent of the data subject for use within an associated or subsequent matter • When bank account and other personal/sensitive data is retained within the firm's intranet in the interests of resisting fraudulent activity The policy is to archive all files and matters as quickly as possible after the conclusion of the transaction but within 6 months in any event which allows a reasonable period for queries, complaints or claims in the aftermath

Special Category Data (continued) **Employees**	of the matter. The policy is to archive files to the firm's intranet which is secure and with the benefit that personal/sensitive data is securely stored. Accordingly, the firm's policy aims at striking a balance between the view that personal/sensitive data should not be retained indefinitely and the layer of protection afforded to both the firm and indeed the firm's clients by retaining data which allows the firm to check ID and bank details and the like and ward off potential fraudulent activity. As to employees and members of staff, the Firm's policy is to retain data for up to 2 years after the employee/member of staff has left the Firm and the Firm's standard contracts of employment reflect that policy and the Firm's employees consent to the same via their contracts.
Review Notes	This policy was reviewed at the Annual Quality Review in September 2021. An incident occurred in February 2019 whereby an attempted fraud was warded off as SRB retained the client's bank and email details and the firm was able to investigate and check an unsolicited payment into the firm's bank account and avoid a repayment to another account which would have amounted to contributing to fraudulent activity. As similar fraudulent activity has been identified in the legal press and by lenders, it is the firm's view that this policy should be altered to allow for the retention of personal and sensitive data which would assist in avoiding possible fraudulent activity. Accordingly, the firm's policy aims at striking a balance between the view that personal/sensitive data should not be

	retained indefinitely and the layer of protection afforded to both the firm and indeed the firm's clients by retaining data which allows the firm to check ID and bank details and the like and ward off potential fraudulent activity. The firm does not rely upon the express consent of its clients in relation to retention of data but relies upon retention in accordance with legitimate and reasonable business purposes. This change of policy is aligned with such legitimate and reasonable business purpose.