AAG Cloud is owned and operated by Class Legal. Class Legal is committed to:

- ensuring that personal data is secured against accidental, unauthorised or unlawful loss, access or disclosure
- identifying reasonably foreseeable and internal risks to security and unauthorised access to personal data
- minimising security risks
- regular testing and
- monitoring for security issues.

The organisational measures the Class Legal has in place are as follows:

Class Legal has implemented a number of policies and procedures to ensure that technical and organisational measures to protect personal data are binding on all staff. Such policies include an incident response plan, data protection policy and other related policies and procedures (such as password protection, authorised access and data protection training) related to the protection of personal data.

Class Legal implements the following measures in relation to personnel security:

- Each member of staff is subject to a contractual obligation of confidentiality. Additional contractual obligations will apply to external personnel in relation to their processing of personal data.
- Staff are subject to appropriate vetting, mandatory training appropriate to their role and corresponding access privileges, security and IT policies and procedures appropriate to their role.

Class Legal implements the following measures around physical security:

- Physical access is limited to individuals whose job responsibilities require them to access that physical location, e.g. a server room will be accessible only by authorised IT personnel, the corporate equipment at the reception will be only accessible by authorised members of staff.
- CCTV is deployed where appropriate.
- Backs up personal data as well as the applications required to read the personal data in accordance with defined schedules and policies. The backup time periods are managed in accordance with industry best practices;
- Utilises a contingency strategy to ensure personal data is available in the event that the primary storage systems go down; and
- Has a recovery plan in place with resources and capacity to recover systems and data in the event of a disaster. Recovery is supervised by appropriate personnel.

Class Legal implements the following controls around supplier security:

- Suppliers are subject to due diligence and appropriate vetting. Where appropriate, a privacy impact (or similar) assessment is carried out to address risks.

- A contract (with, where appropriate, data protection and security obligations) must be put in place with each supplier.
- AAG Cloud operates on a server exclusively owned by Class Legal, housed within Ionos' data centre in the UK. No data is transmitted to any other country.The sole external service utilised is Font Awesome, incorporated for its features; however, users' IP addresses and browser versions are disclosed to the Font Awesome CDN.

The Technical security requirements are as follows:

**Regarding cookies and local storage:**

Our software may issue a cookie to users for identity retention, which is the only cookie generated.

**General user data storage includes:**

- Email addresses and passwords (encrypted in a one-way format) submitted by users.
- The date and IP address of users' acceptance of terms and conditions.
- Anonymous W3C log data.

**Activity-based data storage:**

Users' actions within the system may result in data being stored, linked to their account:

- Entries made in the notepad, possibly accompanied by text notes.
- Pinning of calculators and tools to the homepage.
- Information inputted into calculators, saved as default values for future use.

Although tools like the CSA calculator allow users to input children's names, providing such details is entirely optional.

**Cryptographic Controls:**

User passwords are fortified through a robust encryption process employing a salted, 10,000-iteration PBK-SHA1 algorithm. This ensures that passwords remain inaccessible, even to us.

All user-generated data is securely housed within an MS SQL Server database, residing on the same server as the website itself. Daily database backups are encrypted using GPG and transmitted via SSH. Importantly, storage backups are never stored on a machine with access to the private decryption key, enhancing data security.

**Administration:**

User management is conducted through a distinct, password-protected interface. Administrators are granted access only to users' email addresses and expiry dates, maintaining confidentiality. This administration service remains internal, safeguarding email addresses from exposure to external systems during validation processes.