CAT360 Data Protection Policy

Barbourne Brook Limited

Version 1.0 (new) | Updated: 17 August 2026
This policy is one of the Policies incorporated into the CAT360 Master Software as a Service Agreement (clause 1.2.2(c)).

1. Overview and status of this policy

This Data Protection Policy is one of the Policies incorporated into, and forming part of, each Agreement entered into under the CAT360 Master Software as a Service Terms ("Master SaaS Terms") between Barbourne Brook Limited ("Supplier", "we", "us") and a Customer. It sets out how the Supplier processes personal data in connection with CAT360, and defines terms used elsewhere in the Master SaaS Terms, including Data Protection Losses and Protected Data.

Capitalised terms used in this policy that are not defined here have the meanings given to them in the Master SaaS Terms.

2. Definitions

Data Protection Legislation: the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and any successor or replacement legislation, together with any applicable guidance, codes of practice and determinations issued by the Information Commissioner's Office (ICO) from time to time.

Personal Data, Data Subject, Controller, Processor and Personal Data Breach: have the meanings given in the UK GDPR.

Protected Data: any Personal Data comprised within the Customer Data, and any other Personal Data processed by the Supplier on behalf of the Customer in connection with the Services.

Data Protection Losses: all liabilities, fines, sanctions, interest, penalties, losses, damages, settlements, costs, charges, and legal and other professional fees and expenses of any nature, awarded against, agreed to be paid by, or incurred by a party (whether following a claim by a Data Subject, an investigation or enforcement action by the ICO, or a claim by any other third party), in each case arising out of or in connection with a breach of the Data Protection Legislation, save that Data Protection Losses shall not include any losses excluded under clause 19 (Limitation of liability) of the Master SaaS Terms.

Sub-processor: any third party engaged by the Supplier to process Protected Data on the Supplier's behalf in connection with the Services.

3. Roles of the parties

3.1 In respect of Protected Data comprised within Customer Data, the Customer is the Controller and the Supplier is the Processor. The Supplier processes such Protected Data only on the Customer's documented instructions, including as set out in the Agreement, unless required to do otherwise by law, in which case the Supplier shall (where permitted) inform the Customer of that legal requirement before processing.

3.2 In respect of Account Data relating to Authorised Users (as described in the Privacy Policy), the Supplier acts as Controller.

3.3 Each party shall comply with its own obligations under the Data Protection Legislation applicable to it as Controller or Processor, as the case may be.

4. The Supplier's obligations as Processor

When acting as Processor, the Supplier shall:

- Process Protected Data only on the Customer's documented instructions, unless required otherwise by law.
- Ensure that persons authorised to process Protected Data are subject to a duty of confidentiality.
- Implement appropriate technical and organisational measures to protect Protected Data, as set out in the Information Security Policy.
- Not engage a Sub-processor without the Customer's general authorisation (given by entering into the Agreement), subject to notifying the Customer of any intended changes and giving the Customer a reasonable opportunity to object.
- So far as reasonably possible, assist the Customer by appropriate technical and organisational measures to respond to requests from Data Subjects exercising their rights under the Data Protection Legislation.
- Assist the Customer in meeting its obligations relating to the security of processing, breach notification and data protection impact assessments, taking into account the nature of processing and the information available to the Supplier.
- Notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Protected Data.
- At the Customer's election, delete or return all Protected Data to the Customer after the end of the provision of the relevant Services, and delete existing copies, in accordance with clause 12.6 of the Master SaaS Terms, except to the extent applicable law requires the Supplier to continue to store it.
- Make available to the Customer information reasonably necessary to demonstrate compliance with this section 4.

5. The Customer's obligations

5.1 The Customer warrants that it has all necessary rights and, where applicable, has obtained all necessary consents and notified Data Subjects, to allow the lawful transfer and processing of Customer Data by the Supplier for the purposes of the Agreement, in accordance with clause 9 of the Master SaaS Terms (Customer's responsibilities).

5.2 The Customer shall ensure that its instructions to the Supplier comply with the Data Protection Legislation.

6. International transfers

Where the Supplier or a Sub-processor transfers Protected Data outside the United Kingdom, the Supplier shall ensure appropriate safeguards are in place, such as an adequacy decision, Standard Contractual Clauses, or the UK International Data Transfer Addendum, in accordance with the Data Protection Legislation.

7. Security measures

The technical and organisational measures applied to Protected Data are set out in full in the Information Security Policy, which forms part of the Policies under the Master SaaS Terms. These measures are reviewed at least annually.

8. Data retention and deletion

Protected Data is retained for the duration of the relevant Subscribed Service Period. Unless otherwise agreed in the Proposal or the Subscribed Service Specific Terms, the Supplier will securely dispose of Protected Data within 60 days of the end of the provision of the relevant Services, in accordance with clause 12.6 of the Master SaaS Terms, except where the Supplier is required by UK law to retain it for longer.

9. Personal data breach management

The Supplier maintains a documented incident response process, summarised in the Information Security Policy. Where a Personal Data Breach affects Protected Data, the Supplier will notify the affected Customer without undue delay and provide such information as the Customer reasonably requires to meet its own notification obligations to the ICO and affected Data Subjects.

10. Sub-processors

The Supplier maintains a list of current Sub-processors engaged in connection with CAT360, available to Customers on request. Sub-processors are subject to written contractual terms that impose data protection obligations no less protective than those in this policy.

11. Interpretation and order of priority

This policy forms part of the Policies referred to in clause 1.2.2(c) of the Master SaaS Terms. In the event of any conflict between this policy and the Master SaaS Terms, the order of priority set out in clause 1.2.2 of the Master SaaS Terms shall apply.

12. Review and contact

This policy is reviewed at least annually. Questions about this policy should be directed to Sarah O'Neill, Data Representative, sarah@barbournebrook.co.uk.