



**Smiths Accountancy
Administration Services Ltd**

DATA PROTECTION POLICY

Smiths Accountancy Administration Services Ltd

Company Number	12768440
Office Address	Office 57, Derby West Business Centre, Mackworth, Derbyshire, DE22 4NB

1. PURPOSE OF THIS POLICY

Smiths Accountancy Administration Services Ltd is committed to protecting the privacy, confidentiality and security of all personal information entrusted to us by our clients, employees, suppliers, contractors and other individuals.

This policy explains how the company will collect, use, store, protect and dispose of personal information and sets out the responsibilities of all employees and other individuals working on behalf of the company.

2. LEGISLATION AND REGULATORY FRAMEWORK

Smiths Accountancy Administration Services Ltd will comply with applicable UK data-protection legislation, including the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Data (Use and Access) Act 2025, Privacy and Electronic Communications Regulations (PECR) where applicable, and relevant guidance issued by the Information Commissioner's Office (ICO).

The Data (Use and Access) Act 2025 amended rather than replaced the UK GDPR and Data Protection Act 2018. The ICO confirms that its data-protection provisions are now in force. Where legislation or official ICO guidance changes, this policy will be reviewed and updated as necessary.

3. THE DATA PROTECTION PRINCIPLES

Smiths Accountancy Administration Services Ltd will follow the seven key data-protection principles. Personal information will be:

- Lawful, fair and transparent.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.



**Smiths Accountancy
Administration Services Ltd**

- Accurate and kept up to date where necessary.
- Kept for no longer than necessary.
- Kept secure and confidential.
- Managed with accountability, so the company can demonstrate compliance.

4. PERSONAL INFORMATION WE MAY PROCESS

As an accountancy and administration practice, we may process names and contact details, addresses, telephone numbers, email addresses, dates of birth, National Insurance numbers, tax information, payroll information, salary and employment information, bank and payment information, financial records, business information, identification documents where required, information needed for anti-money laundering and legal compliance, correspondence and other information necessary to provide our services.

Some information may constitute special category or otherwise particularly sensitive personal information. Where this occurs, additional safeguards and an appropriate legal basis will be applied.

5. LAWFUL BASIS FOR PROCESSING

Before processing personal information, Smiths Accountancy Administration Services Ltd will identify an appropriate lawful basis. Depending upon the circumstances, this may include performance of a contract, compliance with a legal obligation, legitimate interests, consent, protection of vital interests or another lawful basis permitted under applicable legislation.

Where consent is relied upon, it will be obtained appropriately and individuals will be informed that they may withdraw consent where applicable.

6. CLIENT CONFIDENTIALITY

All client information must be treated as confidential. Employees must not discuss client information with unauthorised individuals, disclose client information outside the business without appropriate authority, access records without a legitimate business reason, use client information for personal purposes, copy information unnecessarily, leave confidential documents unattended, or remove confidential information from the office unless authorised and appropriate security measures are in place.

Confidentiality obligations continue after an employee leaves the company.



**Smiths Accountancy
Administration Services Ltd**

7. ACCESS TO CLIENT INFORMATION

Access to personal information will be restricted to individuals who require access to perform their role. The company will use appropriate access controls wherever possible, including individual user accounts, strong passwords, appropriate permissions, restricted access to client folders, secure cloud storage, device security and prompt removal of access when an employee leaves or no longer requires access.

Employees must never share passwords or user accounts.

8. EMAIL AND ELECTRONIC COMMUNICATION

Personal and confidential information sent by email must be handled carefully. Employees should check email addresses before sending confidential information, avoid sending information to personal email accounts unless authorised, use secure methods of transmission where appropriate, exercise caution with attachments, report suspected phishing or fraudulent emails, avoid unnecessary personal information in emails and use business email accounts for business communications wherever possible.

9. CLOUD STORAGE AND THIRD-PARTY SYSTEMS

Smiths Accountancy Administration Services Ltd may use third-party software, cloud storage and other service providers to support its business operations. Where another organisation processes personal information on behalf of the company, appropriate contractual and data-protection arrangements will be considered and implemented.

Employees must only use company-approved systems for storing or processing client information.

10. DATA PROTECTION BY DESIGN AND DEFAULT

Data protection will be considered when introducing new systems, software, processes or services. The company will consider what personal information is required, why it is required, who needs access, how long it needs to be retained, risks to individuals, appropriate security measures and whether a less intrusive approach is available.

11. DATA RETENTION

Personal information will only be retained for as long as necessary. Retention periods may be determined by legal, HMRC, professional, contractual, regulatory or legitimate business requirements. When information is no longer required, it will be securely deleted, destroyed or disposed of.



**Smiths Accountancy
Administration Services Ltd**

12. EMPLOYEE RESPONSIBILITIES

Every employee and contractor has responsibility for protecting personal information. Employees must follow this policy, maintain client confidentiality, only access information required for their role, keep passwords secure, lock computers when unattended, report suspected data breaches immediately, follow company procedures, complete required training and ask management if they are unsure how information should be handled.

Failure to follow this policy may result in disciplinary action.

13. DATA BREACHES

A personal-data breach may include sending information to the wrong person, losing paperwork, theft of a laptop or phone, unauthorised access, accidental disclosure, hacking or malware, loss of access to information following a security incident, or any other event resulting in personal information being accidentally or unlawfully lost, destroyed, altered, disclosed or accessed.

All suspected breaches must be reported to management immediately. Employees must not attempt to conceal a breach.

The company will assess each incident and determine whether notification to the ICO or affected individuals is required. Where a reportable personal-data breach is identified, the ICO states that it should generally be reported without undue delay and, where feasible, within 72 hours of becoming aware of it. The company will maintain appropriate records of personal-data breaches and actions taken.

14. INDIVIDUAL RIGHTS

Depending on the circumstances, individuals may have rights including the right to be informed, access, rectification, erasure, restriction of processing, data portability, objection, and rights relating to automated decision-making and profiling where applicable.

Any request relating to an individual's personal information should be passed to management promptly. Employees must not respond to a formal data-protection request independently unless authorised to do so.

15. SUBJECT ACCESS REQUESTS

A Subject Access Request (SAR) is a request by an individual to obtain access to personal information held about them. Employees who receive a request that may constitute a SAR must immediately refer it to management.



**Smiths Accountancy
Administration Services Ltd**

The company will identify and verify the requester where necessary, establish the scope of the request, conduct reasonable and proportionate searches, consider applicable exemptions or restrictions, securely provide the appropriate information and maintain appropriate records of the request and response.

16. DATA PROTECTION COMPLAINTS

Smiths Accountancy Administration Services Ltd will provide individuals with a clear method for raising concerns or complaints about the way their personal information has been handled.

Complaints will be acknowledged within 30 days, investigated appropriately, handled fairly and confidentially, and responded to without undue delay. The company will keep appropriate records of data-protection complaints and corrective action taken.

Where appropriate, individuals will also be informed of their right to complain to the Information Commissioner's Office.

17. PRIVACY NOTICES

Smiths Accountancy Administration Services Ltd will provide appropriate privacy information explaining how personal information is processed. Privacy notices will be reviewed periodically and updated when there are significant changes to processing activities, legislation or regulatory requirements.

Separate privacy notices may be maintained for clients, employees, prospective employees, suppliers and contractors, and website users where appropriate.

18. DIRECT MARKETING

Any direct marketing undertaken by Smiths Accountancy Administration Services Ltd must comply with applicable data-protection and electronic-marketing requirements. Marketing communications will only be sent where there is an appropriate lawful basis and any applicable consent or opt-out requirements have been met. Individuals will be provided with an appropriate opportunity to object to direct marketing.

19. INTERNATIONAL DATA TRANSFERS

Where personal information is transferred outside the UK, Smiths Accountancy Administration Services Ltd will ensure that the transfer is undertaken in accordance with applicable UK data-protection requirements and that appropriate safeguards are used where required.



**Smiths Accountancy
Administration Services Ltd**

20. RECORDS AND ACCOUNTABILITY

The company will maintain appropriate records to demonstrate compliance with data-protection requirements. Depending on the size and nature of the business, these may include records of processing activities, privacy notices, policies, retention schedules, data-breach records, data-protection complaints, staff training records, processor agreements, data-protection impact assessments where required, and records relating to individual rights requests.

21. DATA PROTECTION TRAINING

Employees who handle personal information will receive appropriate information and/or training regarding their data-protection responsibilities. Training may cover confidentiality, secure handling of client information, phishing and cyber security, passwords, email security, data breaches, subject access requests, data retention and the requirements of this policy.

22. MONITORING AND REVIEW

This policy will be reviewed at least annually or sooner where legislation or ICO guidance changes, the company's processing activities materially change, a significant data breach occurs, new software or systems are introduced, or an audit identifies a need for change.

The Directors are responsible for ensuring that this policy remains appropriate and is communicated to staff.

23. ICO COMPLAINTS

Individuals who remain dissatisfied with how their personal information has been handled may raise a concern with the Information Commissioner's Office. Information about making a complaint is available from the ICO.