

Privacy Policy

1. Policy Statement

Stansgate Planning is committed to protecting the privacy and personal data of our clients, employees and consultees. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other applicable data protection legislation.

As a town planning consultancy, we regularly handle personal information relating to planning applicants, landowners, local authority contacts, consultees, employees, and business contacts. We recognise our responsibility to ensure that this information is handled lawfully, fairly, transparently, and securely.

2. Scope

This policy applies to:

- All employees, directors, consultants, and temporary staff.
 - All personal data held by the company in electronic, paper, or other formats.
 - Personal data collected through:
 - Planning applications
 - Land and property assessments
 - Community consultations
 - Website enquiries
 - Client instructions
 - Recruitment activities
 - Business administration activities
-

3. Definition of Personal Data

Personal data means any information relating to an identified or identifiable individual, including:

- Names
- Home addresses
- Email addresses
- Telephone numbers
- Property ownership information
- CVs and employment records
- Financial information
- Photographs
- IP addresses

Special category data (such as health information or information revealing racial or ethnic origin) will only be processed when legally permitted and strictly necessary.

4. Data Protection Principles

The company will ensure personal data is:

Lawful, Fair and Transparent

We will inform clients and staff about how their personal data is used and will rely on an appropriate lawful basis for processing.



Collected for Specified Purposes

Personal data will only be collected for legitimate business purposes.

Adequate and Relevant

We will only collect information necessary for our work and legal obligations.

Accurate

Reasonable steps will be taken to ensure personal data remains accurate and up to date.

Stored for No Longer Than Necessary

Information will be retained only for appropriate business, legal, or regulatory reasons.

Secure

Appropriate technical and organisational measures will be used to protect personal data from loss, misuse, or unauthorised access.

Accountable

The company will demonstrate compliance with data protection legislation through documented procedures and staff awareness.

5. Lawful Bases for Processing

The company processes personal data under one or more of the following lawful bases:

Contract

Where processing is necessary to provide professional planning services to clients.

Legal Obligation

Where processing is required by law or regulatory requirements.

Legitimate Interests

For normal business operations, client relationship management, professional networking, and service improvement, provided individual rights are not overridden.

Consent

Where consent is required, such as certain marketing communications.

6. Types of Data We Process

The company may process:

Client Data

- Contact details
- Property information
- Planning and development proposals
- Correspondence relating to planning projects

Business Contact Data

- Local authority contacts
- Consultees
- Architects
- Surveyors
- Environmental consultants
- Legal advisers



Employee Data

- Personnel records
- Payroll records
- Recruitment documents
- Performance and training records

Website Data

- Enquiry form submissions
- Cookies and analytics information

7. Security Measures

The company will implement appropriate security controls including:

- Password-protected systems and devices
- Multi-factor authentication where available
- Secure cloud storage
- Restricted access to confidential files
- Encryption of sensitive information where appropriate
- Antivirus and software updates
- Secure disposal of paper records
- Regular data backups

Employees must:

- Keep passwords confidential.
- Lock computers when unattended.
- Avoid sharing personal data unnecessarily.
- Report any security concerns immediately.

8. Data Sharing

Personal data will only be shared where necessary and lawful.

This may include:

- Local planning authorities
- Statutory consultees
- Professional advisers
- IT service providers
- Regulatory authorities
- Legal representatives

Where third parties process personal data on our behalf, appropriate contractual safeguards will be in place.

9. Data Retention

The company will retain records only as long as necessary for business, legal, insurance, and professional obligations.

Typical retention periods are:

Record Type	Retention Period
Planning project files	10 years after last invoice date
Clients – sensitive data	24 months from last recorded activity
Financial records	6 years minimum



Recruitment records (unsuccessful applicants)	Immediately after appointment
Employee records – sensitive data	Immediately after employment ends
Employee records – position(s) held and dates of employment	Retained

Records that are no longer required will be securely deleted or destroyed.

10. Individual Rights

Individuals have the right to:

- Access their personal data.
- Request correction of inaccurate information.
- Request erasure of data where applicable.
- Restrict processing.
- Object to processing.
- Request transfer of their data in certain circumstances.
- Withdraw consent where processing is based on consent.

Requests should be submitted to our Data Processor: Sian Holland
Email: sian@stansgate.co.uk

11. Personal Data Breaches

A personal data breach may include:

- Loss of documents containing personal information
- Sending information to the wrong recipient
- Unauthorised access to data
- Malware or cyber incidents

All staff must report suspected breaches immediately to management.

The company will investigate incidents promptly and notify the **Information Commissioner (IC)** and affected individuals where legally required.

12. Training and Responsibilities

All personnel are responsible for:

- Following this policy
- Protecting personal information
- Reporting incidents promptly
- Completing any required data protection training

Management is responsible for monitoring compliance and ensuring appropriate resources are available.

13. Policy Review

This policy will be reviewed annually or sooner if there are significant changes to legislation, technology, or business operations.

