



WILSON JAMES LTD

Artificial Intelligence (AI) Privacy Notice

V1

Artificial Intelligence (AI) Privacy Notice

Title	Artificial Intelligence (AI) Privacy Notice	Date Issued	Sep 2026
Owner	Data Protection Officer (DPO)	Data Reviewed	
Scope	This Policy applies to all sectors and functions of the Wilson James business, all 'workers' and all geographic territories in which Wilson James operates		

1. Purpose

This notice explains how Wilson James uses Artificial Intelligence (AI) technologies and how personal data is processed in connection with those technologies.

We are committed to using AI responsibly, lawfully, transparently and in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and applicable employment, privacy and human rights legislation.

2. Scope

This policy applies to:

- Employees;
- Workers and agency staff;
- Contractors and consultants;
- Job applicants;
- Customers and clients;
- Visitors;
- Suppliers and third parties;
- Any individual whose personal data may be processed through AI-enabled systems used by the organisation.

3. Definition of Artificial Intelligence

For the purposes of this policy, Artificial Intelligence includes systems that can perform tasks that would normally require human intelligence, including but not limited to:

- Automated content generation;
- Meeting transcription and summarisation;
- Document analysis;
- Data classification and organisation;
- Chatbots and virtual assistants;
- Predictive analytics;
- Automated decision-support tools;

- Intelligent search technologies.

AI systems used by the organisation are intended to support human decision-making and operational efficiency and are not a substitute for appropriate human oversight.

4. Our Principles for Using AI

When using AI technologies, the organisation will:

Lawfulness

Ensure that all processing has a valid lawful basis under current data protection legislation.

Transparency

Inform individuals when their personal data may be processed using AI technologies where required.

Fairness

Ensure AI systems do not produce unjustified discriminatory or unfair outcomes.

Data Minimisation

Only process personal data necessary for the specified purpose.

Accuracy

Take reasonable steps to ensure AI-generated outputs are reviewed and verified before significant decisions are made.

Security

Apply appropriate technical and organisational measures to protect personal data.

Human Oversight

Maintain appropriate human review of AI-generated outputs and recommendations.

Accountability

Document and assess AI processing activities, risks and controls.

5. Personal Data We May Process Using AI

Depending on the purpose of processing, AI systems may process:

- Names and contact details;
- Employment information;
- Correspondence and communications;
- Meeting recordings, transcripts and notes;
- Customer interactions;
- Documents and files;
- Operational data;
- System usage information;
- Other personal data provided during normal business activities.

Where special category personal data is processed, additional safeguards and legal requirements will apply.

6. Lawful Bases for Processing

The organisation may rely on one or more of the following lawful bases:

Legitimate Interests

Where AI processing is necessary for legitimate business purposes and those interests are not overridden by the rights and freedoms of individuals.

Examples include:

- Improving operational efficiency;
- Producing meeting notes and summaries;
- Managing knowledge and information;
- Enhancing customer service;
- Maintaining quality assurance processes.

Performance of a Contract

Where processing is necessary to perform contractual obligations.

Legal Obligation

Where processing is required to comply with a legal requirement.

Consent

Where required by law and where consent can be freely given and withdrawn.

7. Use of AI in Employment Matters

The organisation may use AI tools to assist with:

- Drafting documents and correspondence;
- Producing meeting notes or summaries;
- Analysing information;
- Managing workflows;
- Supporting recruitment administration;
- Identifying trends and operational insights.

AI systems will not be used as the sole basis for disciplinary action, dismissal, promotion decisions, performance assessments or any significant employment decision without meaningful human review.

8. Automated Decision-Making

The organisation does not make decisions based solely on automated processing where such decisions produce legal or similarly significant effects on individuals.

If this changes, affected individuals will be informed and provided with information regarding:

- The logic involved;
- The significance of the processing;
- The likely consequences;
- Available rights and safeguards.

9. AI Meeting Recording and Note-Taking

Approved AI note-taking tools may be used in certain meetings to assist with:

- Creating accurate records;
- Producing minutes and action points;
- Supporting business operations;
- Maintaining evidence and audit trails.

Where meetings are recorded or transcribed:

- Participants will normally be informed;
- Access will be restricted to authorised personnel;
- Recordings and transcripts will be retained only as long as necessary;
- Appropriate security controls will be applied.

Additional privacy information may be provided where AI notetaking is used for formal employment processes such as investigations, disciplinary meetings or grievance hearings.

10. Data Protection Impact Assessments

Before introducing AI technologies that may present a high risk to individuals, the organisation will carry out a Data Protection Impact Assessment (DPIA).

The assessment may consider:

- Privacy risks;
- Potential bias or discrimination;
- Data security risks;
- Impacts on individuals' rights and freedoms;
- Measures required to mitigate identified risks.

11. Security Measures

The organisation implements appropriate security measures, including:

- Access controls;
- Authentication measures;
- Encryption where appropriate;
- Monitoring and logging;
- Supplier due diligence;
- Data retention controls.

Only authorised users may access AI systems processing business information.

12. Third-Party AI Providers

Where third-party AI solutions are used, the organisation will take reasonable steps to ensure:

- Appropriate contractual protections are in place;
- Data processing agreements are executed where required;
- Providers offer adequate security standards;
- International transfers comply with UK GDPR requirements.

13. Employee Responsibilities

Employees must:

- Use only authorised AI systems;
- Follow company information security requirements;
- Avoid entering confidential or personal information into unapproved AI platforms;
- Verify AI-generated content before relying upon it;
- Report suspected data breaches immediately.

Failure to comply with this policy may result in disciplinary action.

14. Individual Rights

Individuals have rights under UK GDPR, including:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to object;
- Rights relating to automated decision-making.

Requests should be directed to the Data Protection Officer.

15. Contact Information

Questions regarding the organisation's use of AI in relation to personal data should be directed to:

dataprotection@wilsonjames.co.uk

16. Privacy Notice Review

This notice will be reviewed at least annually and whenever there is a significant change to:

- AI technologies used by the organisation;
- Applicable legislation;
- Regulatory guidance;
- Business processes involving AI.