ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

Document control

- **Organisation:** Berry & Escott Ltd
- **Policy owner:** AI Lead Officer
- **Approved by:** Managing Directors
- **Effective date:** 19 January 2026
- **Review cycle:** Every 12 months, or sooner if law, technology, or risk profile changes

1. Introduction

This policy sets out Berry & Escott Ltd's approach to the use of Artificial Intelligence (AI) across all departments. It ensures responsible, legal, and ethical use of AI in line with UK regulations and our company values.

2. Purpose and Scope

This policy applies to:

- all employees, directors, agency staff, contractors, and third parties working for Berry & Escott Ltd; and
- all uses of AI, including generative AI (text, image, audio, video), analytics, automation, and decision-support tools.

3. Definitions

- **AI:** systems that generate outputs such as predictions, recommendations, content, or decisions.
- **Generative AI:** AI that creates content (text, images, code, audio, video).
- **Personal data:** information relating to an identifiable person.
- **Special category data:** health data, biometric data, religious beliefs, and other protected data under UK GDPR.
- **Confidential information:** non-public company, client, supplier, commercial, technical, pricing, or strategic information.
- **Automated decision-making:** decisions made solely by automated means that have legal or similarly significant effects on individuals.

4. General Principles for AI Use

All AI use must follow these principles:

1. **Human accountability**
   - AI supports decisions. People own decisions.
   - You remain responsible for outcomes, even if an AI suggested them.
2. **Transparency**
   - If AI materially contributed to an output, you must be able to explain how it was used.
   - Do not present AI-generated work as independently verified.
3. **Accuracy and verification**
   - Treat AI like an eager apprentice: useful, fast, and occasionally imaginative.
   - Any facts, standards references, legal claims, or technical assertions must be checked using reliable non-AI sources before use.
4. **Fairness and non-discrimination**
   - AI must not be used in ways that could create discriminatory outcomes.
   - AI must not be used to make decisions about protected characteristics.
5. **Data protection and privacy**
   - Personal data must be processed lawfully, securely, and with data minimisation.
   - Higher-risk processing requires formal assessment (see section 8).
6. **Security**
   - AI use must not introduce cyber, fraud, IP, or information leakage risk.

5. AI Governance and Responsibilities

- **Managing Directors**
  - Provide oversight, ensure resourcing, and approve this policy.
- **AI Lead Officer**
  - Owns AI governance, approves tools, maintains the approved tools list, and leads training.
- **IT / Security Lead**
  - Ensures tools meet security requirements, monitors risk, and supports incident response.
- **Department Heads**
  - Ensure staff follow this policy and that department-specific uses remain controlled.
- **All staff**
  - Follow this policy, complete training, and report concerns or incidents immediately.

6. Approved AI Tools

1. Only tools on the **Approved Tools List (Appendix A)** may be used with company information.
2. New tools must be approved before use. Approval will consider:
   - data protection and security controls;
   - whether the supplier trains models on our data (and opt-out options);
   - data location and retention;

- access control, logging, and admin features;
- commercial terms and IP position.

3. "Free" tools are rarely free. If you are not sure, assume it is not approved and ask.

7. Departmental Guidance

7.1 Sales and Marketing

- Use AI for market analysis, CRM integration, and low risk automated communications.
- Avoid generating false or misleading content.

7.2 Design and Engineering

- Use AI for simulation, drafting, and iterative design support.
- All final designs must be reviewed by qualified engineers.

7.3 Manufacturing Operations

- AI may support predictive maintenance, quality control, and scheduling.
- Human operators must oversee all AI-driven decisions on the production line.

7.4 Human Resources

- Use AI for applicant tracking and HR analytics only if tools are proven to be fair and non-discriminatory.
- Do not use AI to make final decisions on hiring, promotion, or dismissal.

7.5 Finance and Administration

- AI may assist in forecasting, invoice processing, and fraud detection.
- Maintain transparency in any AI-supported financial decisions.

7.6 IT and Data Security

- Monitor AI systems for risks & vulnerabilities and ensure regular patching.

When in doubt: do not paste it. Summarise it in general terms instead.

8. Data protection and risk assessment

AI use involving personal data, monitoring individuals, or decisions affecting individuals must be assessed before use.

You must involve the AI Lead Officer (and where relevant, IT/Security) before any AI use that involves:

- recruitment screening, performance monitoring, or HR analytics;
- customer profiling, credit decisions, or automated approvals;
- CCTV, biometrics, or recognition technologies;
- any processing that is likely to require a DPIA.

Note: UK AI and data protection guidance is evolving following legislative updates, so we will update this policy and supporting guidance as needed. (ICO)

9. Acceptable use

AI can be used for:

- drafting and improving text that does not include confidential or personal data;
- summarising meeting notes where content is non-sensitive;
- brainstorming, planning, and checklists;
- assisting with internal process improvement;
- non-sensitive marketing ideation (final claims must be verified).

10. Prohibited use

AI must not be used to:

- generate or distribute illegal, abusive, or harmful content (including deepfake intimate images);
- create misleading content, fake endorsements, or fabricated "evidence";
- bypass security controls, write malware, or assist wrongdoing;
- make final automated HR decisions on hiring, promotion, or dismissal;
- make decisions about protected characteristics.

11. Breaches and Disciplinary Action

Breaches of this policy may result in:

- investigation,
- disciplinary action under company procedure, and
- regulatory reporting where required.

12. Cross-Referencing with Other Policies

This policy should be read in conjunction with:

- Disciplinary Policy
- Grievance Policy
- Data Protection Policy
- Equality Policy

13. Appendix A: Approved AI Tools

- Gamma
- ChatGPT Teams
- Perplexity Pro
- Markmap
- Notebook LM

- Excalidraw

(Note: All tools are approved as of January 2026 and are subject to periodic review.)

14. Glossary of Terms

- AI (Artificial Intelligence): Technology that enables machines to mimic human decision-making.
- Bias: Systematic error resulting in unfair outcomes.
- GDPR: General Data Protection Regulation.
- ICO: Information Commissioner's Office.
- Personal Data: Any information relating to an identifiable person.
- Transparency: Clear and open explanation of processes.

The Managing Directors will ensure the effective implementation of this Policy. This policy is freely available to all interested parties.

L. Berry

Director

C. Escott

Director/

AI Lead Officer

Reviewed and signed 21st January 2026