

Copperstone Projects

Artificial Intelligence (AI) Policy

Document Owner: Directors, Copperstone Projects

Applies To: All employees, subcontractors, consultants, temporary workers, and third-party suppliers using AI tools on behalf of Copperstone Projects

Version: 2.0

Effective Date: May 2026

Review Frequency: Annual or following significant regulatory or operational changes

1. Purpose

Copperstone Projects recognises that Artificial Intelligence (AI) technologies can improve productivity, project delivery, safety, communication, administration, and operational efficiency across the construction and building contracting sector.

This policy sets out how AI systems may be used responsibly, securely, legally, and ethically within Copperstone Projects.

The objectives of this policy are to:

- Encourage safe and productive use of AI tools;
- Protect confidential company and client information;
- Ensure compliance with UK laws and regulations;
- Maintain professional standards and human accountability;
- Reduce risks associated with inaccurate, biased, or insecure AI outputs;
- Ensure AI use aligns with Copperstone Projects' commercial, legal, and safety obligations.

2. Scope

This policy applies to:

- All employees;
- Directors and managers;
- Site managers and project teams;
- Office staff;
- Consultants and subcontractors using company systems or data;
- Any AI system accessed using company devices, systems, email accounts, or company information.

This policy applies to both:

- Public AI tools (e.g. ChatGPT, Microsoft Copilot, Gemini, Claude);
- Specialist construction or project-management AI software integrated into business systems.

3. Definition of Artificial Intelligence

For the purpose of this policy, AI refers to software systems capable of generating content, analysing information, automating tasks, making predictions, or assisting with decision-making using machine learning, large language models, or similar technologies.

Examples include:

- AI writing assistants;
- Meeting summarisation tools;
- AI-enabled estimating software;
- AI image or drawing generation tools;
- AI scheduling or planning systems;
- AI chatbots;
- AI-powered document review systems.

4. Guiding Principles

Copperstone Projects will use AI in accordance with the following principles:

4.1 Human Oversight

AI tools are assistive technologies only. Final responsibility for decisions, communications, designs, estimates, procurement, contractual matters, and safety remains with appropriately qualified personnel.

4.2 Confidentiality

Company, client, supplier, employee, and project information must be protected at all times.

4.3 Accuracy

AI-generated outputs must always be reviewed and verified before use.

4.4 Compliance

AI use must comply with:

- UK GDPR and Data Protection Act 2018;
- Construction industry regulations;
- Contractual confidentiality obligations;
- Copyright and intellectual property laws;
- Health and safety legislation;
- Company IT and cybersecurity policies.

4.5 Fairness and Professionalism

AI must not be used in ways that are discriminatory, misleading, unethical, or damaging to clients, employees, suppliers, or the company's reputation.

5. Approved Uses of AI

The following uses of AI are generally permitted where reasonable care and oversight are maintained.

5.1 Administrative Support

AI may be used for:

- Drafting emails;
- Summarising meeting notes;
- Producing first drafts of reports;
- Creating presentation materials;
- Formatting documents;
- Generating internal templates.

5.2 Project Management Support

AI may assist with:

- Programme drafting;
- Risk register templates;
- Action tracking;
- Progress reporting;
- Procurement summaries;
- Document organisation.

5.3 Estimating and Commercial Functions

AI may support:

- Quantity take-off assistance;
- Cost comparison exercises;
- Draft tender responses;
- Contract review support.

However, all outputs must be independently verified by competent personnel.

5.4 Health and Safety Administration

AI may assist in:

- Drafting RAMS templates;
- Toolbox talk outlines;
- Safety communication drafts;
- Incident report formatting.

AI-generated health and safety content must always be reviewed and approved by qualified personnel before use on site.

5.5 Marketing and Business Development

AI may be used for:

- Social media drafts;
- Website content;
- Case studies;
- Bid support documentation;
- Marketing imagery.

Any published content must be reviewed for accuracy and professionalism.

6. Prohibited Uses of AI

The following uses are prohibited unless specifically authorised in writing by management.

6.1 Uploading Confidential Information

Users must not upload or enter the following into public AI systems unless approved and secured:

- Client confidential information;
- Tender pricing;
- Contract documents;
- Legal advice;
- Financial information;
- Personal data;
- Employee records;
- Site security information;
- Drawings marked confidential;
- Commercially sensitive project details.

6.2 Fully Automated Decision-Making

AI must not make unsupervised decisions relating to:

- Employment;
- Recruitment;
- Disciplinary actions;
- Health and safety decisions;
- Contractual approvals;
- Financial authorisations;
- Supplier selection.

6.3 Unsafe or Unverified Technical Outputs

AI must not be relied upon for:

- Structural calculations;
- Engineering certification;
- Building regulation compliance confirmation;

- Fire safety assessments;
- Temporary works design;
- CDM compliance decisions;
- Legal advice.

Professional review by qualified individuals is mandatory.

6.4 Misrepresentation

Employees must not:

- Present AI-generated content as independently authored expertise where misleading;
- Use AI to impersonate individuals;
- Create false records or documents;
- Generate deceptive imagery or communications.

6.5 Copyright or Intellectual Property Infringement

AI tools must not be used to knowingly reproduce copyrighted content or proprietary designs without permission.

7. Data Protection and Confidentiality

7.1 GDPR Compliance

All AI use involving personal data must comply with UK GDPR and the Data Protection Act 2018.

Personal data must not be entered into AI tools unless:

- The tool has been approved by management or IT;
- Appropriate safeguards are in place;
- Data processing obligations have been assessed.

7.2 Client Confidentiality

Confidential client information must never be shared with unapproved AI systems.

Employees are responsible for ensuring contractual confidentiality obligations are maintained.

7.3 Information Security

Only approved AI platforms may be installed or connected to company systems.

Employees must:

- Use strong passwords and multi-factor authentication where available;
 - Avoid sharing company credentials with AI systems;
 - Report suspected data breaches immediately.
-

8. Accuracy and Verification

AI systems can generate inaccurate or misleading outputs (“hallucinations”).

Accordingly:

- All AI-generated content must be reviewed by a competent person;
- Technical information must be independently verified;
- Contractual and commercial information must be checked before issue;
- Safety-related outputs require formal review.

No employee may rely solely on AI-generated information when making business-critical decisions.

9. Intellectual Property and Ownership

Unless otherwise agreed:

- Work created by employees using AI in the course of employment remains the property of Copperstone Projects;
 - Employees must ensure AI-generated outputs do not infringe third-party intellectual property rights;
 - Employees must not upload proprietary company documents into unapproved external systems.
-

10. Procurement and Approval of AI Tools

No employee may:

- Purchase AI software;
- Subscribe to AI services;
- Integrate AI tools with company systems;
- Connect AI tools to company email, project management, or document systems;

without prior approval from management.

All new AI tools should be assessed for:

- Security;
- GDPR compliance;
- Data storage location;
- Commercial risk;
- Accuracy;
- Vendor reputation;
- Cybersecurity standards.

11. Use of AI in Health and Safety

Copperstone Projects prioritises safety above operational efficiency.

AI must never replace:

- Site supervision;
- Competent health and safety advice;
- Formal risk assessments;
- Engineering judgement;
- Legal compliance checks.

Any AI-assisted health and safety documentation must be reviewed and approved by competent personnel before implementation.

12. Monitoring and Auditing

Copperstone Projects reserves the right to:

- Monitor use of company systems;
- Audit AI usage where necessary;

- Restrict or remove access to AI tools;
- Investigate misuse of AI systems.

Monitoring will be carried out in accordance with applicable laws and company policies.

13. Training and Awareness

Employees using AI tools may receive training covering:

- Appropriate AI usage;
- Cybersecurity risks;
- Data protection obligations;
- AI limitations and risks;
- Verification requirements;
- Responsible prompting practices.

Managers are responsible for ensuring their teams understand this policy.

14. Reporting Concerns

Employees must report immediately if they become aware of:

- Suspected AI-related data breaches;
- Inaccurate or unsafe AI outputs;
- Misuse of AI systems;
- Confidential information exposure;
- Security concerns relating to AI tools.

Reports should be made to:

- A Director;
 - Line management; or
 - The company's IT or compliance contact.
-

15. Breaches of this Policy

Failure to comply with this policy may result in:

- Removal of access to systems;
- Disciplinary action;
- Contract termination;
- Legal action where appropriate.

Serious breaches involving confidential information, safety risks, or unlawful conduct may be treated as gross misconduct.

16. Roles and Responsibilities

Directors

Directors are responsible for:

- Approving AI strategy and governance;
- Ensuring legal compliance;
- Reviewing high-risk AI use.

Managers

Managers are responsible for:

- Ensuring staff understand this policy;
- Monitoring appropriate AI use within teams;
- Escalating concerns.

Employees and Users

Users are responsible for:

- Following this policy;
 - Protecting confidential information;
 - Verifying AI outputs;
 - Using AI professionally and responsibly.
-

17. Future Regulatory Compliance

Copperstone Projects acknowledges that AI regulation is evolving.

The company will review and update this policy periodically to reflect:

- UK legislation;
- ICO guidance;
- Construction industry best practice;
- Cybersecurity developments;
- Client requirements.

18. Policy Review

This policy will be reviewed:

- At least annually; or
- Following significant changes in technology, law, business operations, or security requirements.

Appendix A – Practical Rules for Employees

DO

- Use AI to improve efficiency and drafting;
- Double-check all outputs;
- Keep confidential information secure;
- Ask management if unsure;
- Use approved tools only.

DO NOT

- Upload confidential documents into public AI tools;
 - Rely on AI for technical or legal sign-off;
 - Use AI to make employment decisions;
 - Share personal data improperly;
 - Assume AI outputs are correct.
-

Appendix B – Example Approved AI Use Cases

Area	Example Use
Administration	Drafting meeting summaries
Project Management	Creating action trackers
Estimating	Tender response structuring
Health & Safety	Draft toolbox talks
Marketing	Social media and website copy
Commercial	Contract clause summaries

Appendix C – Example High-Risk AI Uses Requiring Approval

- AI integration with project management systems;
 - AI analysis of employee data;
 - AI-enabled CCTV or monitoring systems;
 - Automated recruitment screening;
 - AI systems processing client personal data;
 - AI-generated technical design outputs.
-

Acceptance

All employees and relevant contractors are expected to read, understand, and comply with this policy.

Questions regarding this policy should be directed to company management.