Cornerstone Nurseries
Artificial Intelligence (AI) Accepted Use Policy

Purpose

This policy sets out our organisational approach to the responsible, lawful, ethical and secure use of Artificial Intelligence (AI) technologies.

Cornerstone Nurseries recognises that AI tools can improve productivity, efficiency and innovation. However, their use may also create risks relating to confidentiality, data protection, employment relations, intellectual property, accuracy, bias and reputational damage.

This policy applies to all employees, workers, contractors, consultants, agency staff, volunteers and any other individuals engaged by the organisation.

This policy applies to:

- Generative AI tools (including but not limited to: ChatGPT, Claude, Gemini, Copilot and similar technologies)
- AI-powered writing, summarisation and transcription tools
- AI image, video and audio generation tools
- AI-enabled recruitment, assessment or screening tools
- AI-powered productivity applications
- Any future AI systems adopted by the organisation

This policy applies whether AI systems are accessed through organisational devices, personal devices, web-based platforms or integrated software applications.

Guiding Principles

The organisation's use of AI shall be:

Lawful

Complying with UK legislation, including:

- UK GDPR
- Data Protection Act 2018
- Equality Act 2010
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988

- Employment Rights Act 1996
- Common law duties of confidentiality

Transparent
Individuals should understand when AI has materially contributed to content, decisions or outputs.

Accountable
Responsibility for decisions remains with humans and cannot be delegated to AI systems.

Fair
AI must not be used in a way that creates unlawful discrimination or unfair treatment.

Secure
Confidential, personal and commercially sensitive information must be protected at all times.

Definitions
For the purpose of this policy:

- **Artificial Intelligence (AI)**
  Computer systems capable of generating content, analysing information, making recommendations or performing tasks that would normally require human intelligence.
- **Generative AI**
  AI systems capable of creating text, images, audio, video, code or other content.
- **Personal Data**
  Any information relating to an identified or identifiable individual.
- **Special Category Data**
  Personal data requiring enhanced protection, including information relating to health, ethnicity, religion, trade union membership, sexual orientation or biometric data.

Permitted Uses

Subject to this policy, employees may use approved AI tools for:

- Drafting routine correspondence
- Producing first drafts of reports
- Research and information gathering
- Summarising documents
- Creating meeting agendas
- Generating ideas and brainstorming
- Formatting content
- Producing training materials
- Administrative support tasks

All AI-generated outputs must be reviewed by a competent human before use.

Prohibited Uses

Employees must not:

Upload or disclose confidential information

- Confidential business information
- Client or customer information
- Commercially sensitive information
- Trade secrets
- Legal advice
- Financial data
- Internal investigation materials

unless expressly authorised and approved for use within a secure organisational AI system.

Upload Personal Data

Employees must not enter personal data into public AI systems without explicit authorisation and a lawful basis under UK GDPR.

This includes:

- Employee information
- Applicant information
- Customer information
- Medical information
- Disciplinary records
- Grievance information

Make Employment Decisions

AI must not independently make decisions relating to:

- Recruitment
- Promotion
- Dismissal
- Redundancy
- Disciplinary action
- Performance management
- Grievances
- Capability processes

Human decision-makers remain accountable for all employment decisions.

Create Misleading Content

Employees must not use AI to:

- Create false records

- Fabricate evidence
- Misrepresent facts
- Impersonate another individual
- Generate discriminatory or offensive material

AI-Assisted Employment Relations Documents

The organisation recognises that employees may use AI tools to assist with drafting workplace documents.

Examples include:

- Grievances
- Appeals
- Flexible working requests
- Complaints
- Statements
- Correspondence

The use of AI assistance is not prohibited, however:

- Employees remain responsible for the accuracy and truthfulness of all submissions.
- Documents must genuinely reflect the employee's own experiences and concerns.
- The organisation may seek clarification where submissions appear inconsistent, generic or unclear.
- The organisation will assess the substance of concerns raised rather than the quality or sophistication of drafting.

No employee will be disadvantaged solely because they have used AI assistance when preparing a workplace document.

Use of AI by Managers

Managers must not rely solely upon AI-generated recommendations when:

- Conducting investigations
- Assessing evidence
- Determining credibility
- Managing performance
- Conducting disciplinary processes
- Considering grievances
- Selecting employees for redundancy

Managers must exercise independent judgement and document decision-making processes.

Data Protection and GDPR

All use of AI must comply with UK GDPR and the Data Protection Act 2018.

Employees must:

- Process personal data lawfully, fairly and transparently.
- Use only approved systems for processing personal data.
- Follow organisational data protection procedures.
- Report any suspected data breaches immediately.

Special category data must never be entered into public AI systems without specific approval and safeguards.

Intellectual Property and Copyright

Employees must ensure that:

- AI-generated content does not infringe copyright.
- Third-party intellectual property rights are respected.
- Organisational intellectual property remains protected.

Any work product created during employment remains subject to organisational ownership

Accuracy and Verification

AI systems can produce inaccurate, incomplete or misleading information.

Employees must:

- Verify factual information.
- Check references and sources.
- Review calculations and analysis.
- Exercise professional judgement.

AI outputs must not be treated as authoritative without verification.

Bias, Equality and Inclusion

AI systems may reflect biases contained within training data.

Users must remain alert to:

- Discriminatory outputs
- Stereotyping
- Inappropriate assumptions
- Unfair treatment of protected groups

Any concerns should be reported immediately.

Social Media and External Communications

The organisation's Social Media Policy applies equally to AI-generated content.

Employees must not:

- Present AI-generated content as official organisational communications without approval.
- Publish confidential information.
- Create misleading public statements.
- Generate content that may damage the organisation's reputation.

Monitoring and Auditing

The organisation reserves the right to:

- Monitor use of organisational systems.
- Audit use of approved AI tools.
- Investigate suspected misuse.
- Restrict access to AI applications where necessary.

Monitoring will be conducted in accordance with applicable privacy and employment laws.

Training

Employees using AI systems may be required to complete training covering:

- Responsible AI use
- Data protection
- Information security
- Ethical considerations
- Equality and bias awareness

Reporting Concerns

Employees should report concerns relating to:

- Data breaches
- Inaccurate outputs
- Discrimination or bias
- Security issues
- Unauthorised AI use

Reports should be made to a line manager, HR, Information Governance Lead or Data Protection Officer as appropriate.

Breach of Policy

Failure to comply with this policy may result in:

- Withdrawal of AI access
- Informal management action
- Disciplinary action
- Termination of engagement where appropriate

Serious breaches involving confidentiality, data protection or deliberate misuse may be treated as gross misconduct.

Policy Review

This policy will be reviewed annually or sooner where there are significant legal, technological or organisational developments.

19/06/26 CJS Review Annually