

ARTIFICIAL INTELLIGENCE POLICY



Policy Review					
Author/Owner	Position	Approved by: Signature:	Approval Date	Review Cycle Review Date	Published on Website Y/N
Emma Cox	Vice Principal Infrastructure & Projects/Digital	Chair of Corporation 	SLT: 06.07.26 Corp: 16.07.26	Annually July	Y

Document Control – Revision History (Policies only)					
Author/Owner	Summary of Changes	Date	Date last reviewed by SED	Version	Recommend to SED Y/N
Emma Cox	New Policy	09/06/2026	N/A	1	Y

Initial Equality Impact Screening

Has anyone else been consulted on this policy and/or procedure? Yes, SLT, Safeguarding, Student Services, Equality & Diversity and wider digital stakeholder groups

What evidence has been used for this impact screening (e.g. related policies, publications)?

Declaration (please tick one statement and indicate any negative impacts)

☒ I am satisfied that an initial screening has been carried out on this Policy and/or Procedure and a full Equality Impact Assessment is not required. There are no specific negative impacts on any of the Protected Characteristics groups.

☐ I recommend that an Equality Impact Assessment is required by the Equality and Diversity group, as possible negative impacts have been identified for one or more of the Protected Characteristics groups as follows:

- ☐ Age
- ☐ Disability
- ☐ Gender Reassignment
- ☐ Race
- ☐ Religion or belief
- ☐ Sex
- ☐ Sexual orientation
- ☐ Marriage & civil partnership
- ☐ Pregnancy & maternity

Completed by:	Mark Bolton	Position:	Principal	Date:	July 2026
----------------------	-------------	------------------	-----------	--------------	-----------

Reviewed by Equality & Diversity Group: YES If Yes: Date: 09.05.18

I confirm that any recommended amendments have been made

Summary of Comments including Recommendations from Equality & Diversity Group Review:

Amended by Author:		Position:		Date:	
---------------------------	--	------------------	--	--------------	--

Contents

1. AIMS 3

2. SCOPE..... 3

3. GUIDING PRINCIPLES 3

4. DISTRIBUTION 5

5. RESPONSIBILITY AND AUTHORITY 5

6. RISK MANAGEMENT 6

7. TRAINING AND DEVELOPMENT 6

8. BREACHES AND MISUSE..... 6

9. RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS..... 7

10. DEFINITIONS..... 8

Appendix 1 – List of Approved AI Tools10

1. AIMS

Yeovil College recognises that Artificial Intelligence is already reshaping education, employment, public service and business operations. Used appropriately AI presents significant opportunities to enhance teaching, learning, business efficiency and student outcomes.

The College also recognises that AI presents risks, including inaccurate or biased outputs, inappropriate reliance on automated systems, academic misconduct, data protection breaches, safeguarding concerns, intellectual property infringement and cyber security threats.

The College adopts a position of 'cautious optimism', and sets out the college's expectation for responsible, ethical, transparent while ensuring innovation takes place with clear compliance and robust safeguards are in place.

2. SCOPE

- 2.1. This policy applies to all AI use connected with Yeovil College, including teaching, learning, assessment support, learner support, administration, business operations, communications, research, content creation, data analysis and innovation activity.
- 2.2. It applies to all staff, learners, governors, contractors, consultants, volunteers, agency staff, visitors and third parties working on behalf of the College.
- 2.3. It applies to standalone AI tools, AI-enabled features within wider systems, generative AI tools, transcription tools, chatbots, adaptive learning platforms, predictive tools, automated workflows and any other system that uses AI to generate, classify, summarise, recommend, analyse or support decision-making.

3. GUIDING PRINCIPLES

Yeovil College's approach to AI is guided by the following principles:

3.1 Safe and Responsible Use

AI must be used in a way that is:

- Lawful, ethical and transparent
- Secure and compliant with College policies
- Respectful of individuals and communities

This reflects the College's broader requirement to process information lawfully, fairly and securely.

3.2 Cautious Innovation

The College encourages experimentation with AI where it:

- Enhances teaching and learning
- Improves student experience

- Drives operational efficiency

However, all innovation must take place within approved frameworks and governance structures.

3.3 Approved Tools and Environments

- The Technology in Learning Group will maintain and publish a list of approved AI tools and applications, please see Appendix A [LINK].
- Priority will be given to enterprise, secure platforms, with Microsoft Copilot as the primary AI tool.
- Use of unapproved or free/open AI tools for College work is restricted where data or IP is involved.

3.4 Data Protection and Security

No AI tool may be used to process:

- Personal data
- Special category data
- Sensitive College, commercial or safeguarding information

Unless:

- The tool is approved, and
- A Data Protection Impact Assessment (DPIA) has been completed where required

This aligns with the requirement to ensure secure processing and minimise risk to personal data.

3.5 Intellectual Property Protection

Staff and learners must ensure:

- College IP is not uploaded into unsecured AI tools
- AI-generated content does not infringe third-party rights
- Outputs created using AI remain compliant with College IP expectations

In line with the College's position that IP created through College activity must be protected and managed appropriately.

3.6 Safeguarding and Wellbeing

AI must not be used in ways that:

- Compromise safeguarding processes
- Introduce risk to vulnerable learners

- Generate harmful, inappropriate or unsafe content

The College maintains zero tolerance for safeguarding risk as part of its overall risk appetite.

3.7 Academic Integrity and Student Behaviour

Learners must:

- 3.7.1 Use AI tools only where permitted by staff
- 3.7.2 Not submit AI-generated work as their own unless explicitly allowed
- 3.7.3 Follow all guidance relating to plagiarism and academic misconduct
- 3.7.4 Follow all awarding body guidelines
- 3.7.5 Misuse of AI will be treated in line with:
- 3.7.6 Learner disciplinary procedures
- 3.7.7 Academic misconduct processes

3.8 Staff Professional Use

Staff may use AI to support:

- 3.8.1 Curriculum planning.
- 3.8.2 Resource creation.
- 3.8.3 Administrative efficiency
- 3.8.4 Innovation in pedagogy

However, staff must ensure:

- 3.8.5 Outputs are reviewed and validated (AI should not replace professional judgement or subject matter expertise).
- 3.8.6 AI does not replace the role of the teacher.
- 3.8.7 AI should not be used to make assessment decisions.
- 3.8.8 AI Transcription, Recording and Meeting Summaries - must only be used where all participants have been informed in advance and the use has been approved. Staff must explain the purpose of the transcription or summary, how the output will be used, where it will be stored and who will have access. Transcripts, recordings or AI-generated summaries containing personal data, confidential information or sensitive matters must not be shared outside the College unless there is a lawful basis, appropriate approval and secure transfer arrangements.
- 3.8.9 Decisions are not automated.
- 3.8.10 All use aligns with College policies.

4. DISTRIBUTION

This policy is available on Yeovil College's website and in hard copy from the college.

5. RESPONSIBILITY AND AUTHORITY

5.1 Digital Innovation Project Group

Responsible for:

- Exploring emerging AI opportunities
- Supporting pilot projects and innovation
- Evaluating strategic impact

- Publishing approved list of AI Tools (Appendix 1)

5.2 Technology in Learning Group

Responsible for:

- Approving AI tools and platforms
- Publishing the approved tools list
- Providing guidance to staff

5.3 Senior Leadership Team

Responsible for:

- Strategic oversight
- Risk management
- Policy approval and review

5.4 All Staff and Users

Responsible for:

- Complying with this policy
- Reporting concerns or misuse
- Using AI tools responsibly

6. RISK MANAGEMENT

AI-related risks will be managed through:

- Existing risk management frameworks
- Data protection processes (including DPIAs)
- IT security controls
- Staff training and awareness

This aligns with the College's approach of embedding risk management into planning and operations.

7. TRAINING AND DEVELOPMENT

The College will:

- Proportionate AI literacy training to staff and, where appropriate, learners.
- Provide guidance and training on AI tools.
- Support staff to develop AI literacy and capability.
- Promote best practice in teaching and learning.

8. BREACHES AND MISUSE

Failure to comply with this policy may result in:

- Removal of system access.

- Disciplinary action (staff or learners).
- Referral to safeguarding or external agencies where appropriate.

This reflects the expectation that misuse of digital systems may result in disciplinary action.

Where personal data may have been compromised, the Data Protection Officer must be informed immediately so that breach assessment, containment and regulatory timescales can be managed.

9. RELATED POLICIES, PROCEDURES, DOCUMENTS, DEFINITIONS

This policy should be read alongside the following College policies, procedures and guidance where relevant:

- Data Protection Policy
- Acceptable Use of IT Policy
- Records Retention Policy
- Safeguarding and Prevent Policy
- Learner Disciplinary Policy & Procedure
- Disciplinary & Grievance Policy (Staff)
- Academic Misconduct Procedure
- Internal Verification Procedures
- Freedom of Information Policy
- Equality, Diversity and Inclusion Policy & Procedure
- Business Code of Conduct
- Learner Code of Conduct
- Digital Strategy
- Approved AI Tools – Appendix A

Related external legislation and guidance

This policy is informed by, and should be applied consistently with, relevant external requirements including:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Equality Act 2010
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Keeping Children Safe in Education
- Department for Education guidance on generative AI in education
- Information Commissioner's Office guidance on AI and data protection
- Information Commissioner's Office guidance on automated decision-making and profiling
- Joint Council for Qualifications guidance on AI use in assessments
- Awarding body rules and qualification-specific assessment requirements
- Office for Students guidance

10. DEFINITIONS

For the purposes of this policy and guidance:

Term	Definition
Artificial Intelligence / AI	Technologies or systems that perform tasks normally associated with human intelligence, such as generating content, analysing data, recognising patterns, making predictions, classifying information, summarising content or supporting decisions.
Generative AI	AI that creates new content such as text, images, audio, video, code, summaries, lesson materials, reports, feedback or communications in response to prompts or instructions.
AI tool	Any standalone application, embedded system feature, chatbot, digital assistant, transcription tool, adaptive platform, automated workflow, recommendation system or software function that uses AI.
Approved AI tool	An AI tool that has been assessed and approved by the College for specified purposes and is included on the approved AI tools list or AI inventory.
Unapproved AI tool	Any AI tool that has not been formally approved by the College, or which is being used outside its approved purpose or conditions.
Personal data	Information relating to an identified or identifiable living individual, including names, contact details, learner records, staff records, images, voice recordings, opinions or identifiers.
Special category data	More sensitive personal data requiring additional protection, including information about health, ethnicity, religion, political opinions, trade union membership, biometric data, genetic data, sex life or sexual orientation.
Confidential information	Information that is not intended for public disclosure, including College business information, contracts, safeguarding information, HR records, legal advice, financial information, internal reports and commercially sensitive material.
Prompt	Information, instruction, question, file or content entered into an AI tool to generate or influence an output.
AI output	Content, recommendation, summary, analysis, response, prediction, classification, image, audio, transcript, code or other result generated by an AI tool.
Automated decision-making	A decision made solely by automated means without meaningful human involvement.
Profiling	Automated processing of personal data to evaluate, analyse or predict aspects of an individual, such as performance, behaviour, attendance, risk, preferences or needs.

Human oversight	Meaningful review, challenge and accountability by a staff member before AI-assisted content, recommendations or outputs are used or relied upon.
DPIA	A Data Protection Impact Assessment used to identify and manage privacy risks where processing is likely to result in high risk to individuals.
AI inventory	A record of approved AI tools, permitted uses, owners, risk ratings, DPIA status, review dates and restrictions.
Hallucination	An AI-generated output that appears plausible but is inaccurate, fabricated, misleading or unsupported by reliable evidence.
Bias	An unfair or inappropriate tendency in AI outputs, recommendations or decisions that may disadvantage individuals or groups.
Deepfake	AI-generated or manipulated audio, image or video content that appears to show a person saying or doing something they did not say or d

Appendix 1 – List of Approved AI Tools

AI Tool	Use Data	Use IP	Use for Teaching Planning	Use for Learner Resource Production	Use for Assessment
Copilot - Enterprise	P	P	P	P	X
Claude	X	X	P	P	X
Perplexity	X	X	P	P	X
Chat GPT	X	X	P	P	X
Quizlet	X	X	P	P	X
Gemini	X	X	P	P	X
Notebook LM	X	X	P	P	X
Slido	X	X	P	P	X
Grammarly	X	X	P	P	X
Miro Board	X	X	P	P	X