



Blessed Christopher Wharton Catholic Academy Trust
(BCWCAT)

AI in Education Policy

Document Control

1. **Author:** Director of Information Technology
2. **Accountable Executive:** CEO
3. **Reviewers:** DPO, DSLs, Headteachers, HR Lead, IT Director
4. **Applies to:** All staff, volunteers, contractors, students (as directed), governors
5. **Review cycle:** Annual, or sooner on material change to law/DfE guidance
6. **Next review:** September 2026

Purpose & Ethos

BCWCAT will harness AI to improve teaching, learning and operational efficiency without compromising safeguarding, dignity, or human judgment.

Our approach is rooted in the Catholic ethos: technology must serve the common good, equity, truth, and each child's flourishing.

Alignment:

- DfE Safe and Effective Use of AI (Modules 1–4) and leadership toolkit framing
- KCSIE online safety
- UK GDPR
- ICO Children's Code
- Online Safety Act 2023
- Equality Act 2010
- JCQ/Ofqual on academic integrity.

Scope

People: All staff, supply, trainees, volunteers, contractors, governors; pupils only under staff direction.

Uses: Any AI (incl. generative AI) used for curriculum, assessment, administration, or communication, Trust-hosted or third-party.

Data: Any processing of staff/pupil data with/through/by AI systems.

Definitions (plain English)

- **AI:** Software that undertakes tasks associated with human intelligence (pattern recognition, language understanding).
- **Generative AI (GenAI):** Creates new content (text, images, audio, video, code) from prompts.
- **LLM:** Large language model behind many chat assistants.
- **Automated decision-making (ADM):** Decisions about a person made by machines without meaningful human involvement (restricted under GDPR Article 22).

Principles

- **Safeguarding first:** No AI use where child risk isn't demonstrably mitigated; logs retained per schedule.
- **Human in the loop:** AI supports; it never replaces professional judgment or teacher–pupil relationships.
- **Transparency:** Staff/students disclose significant AI contributions in work.
- **Data minimisation:** Avoid entering personal/sensitive data; where necessary, do a DPIA and get DPO sign-off.

- **Equity & inclusion:** Use AI to support SEND accessibility, not widen gaps, and meet PSED duties.

Roles & Responsibilities

Role	Responsibilities
Trust Board	Approves policy; receives annual AI Risk & Safeguarding Report .
CEO & Executive	Strategic direction; resources; compliance.
IT Director (AI Lead)	Maintains Approved AI Tools Register ; configures filtering/monitoring; coordinates training; oversees audits.
DPO	DPIAs; vendor DPAs; privacy notices; incident response.
DSLs / Online Safety Leads	AI-related safeguarding oversight; incidents; parent comms.
Headteachers	Local implementation; compliance; audits; community comms.
All Staff	Complete mandated training; use only approved tools; critically review outputs; follow data/IP/assessment rules; report incidents.
Students	Use only as permitted; disclose assistance; follow Pupil AI Code; protect privacy; report concerns.

Training & Access

- **Mandatory:** Staff complete DfE Modules 1–4 (Leadership/Staff editions) before using AI in teaching/admin; refresher every 2 years or on guidance changes. Permission to use AI is granted only once completion is recorded.

For staff convenience we have combined all the AI DfE modules into one PowerPoint presentation, please request the latest file from your school business manager or by emailing ai@bcwcat.co.uk

- **Student induction:** Age-appropriate AI literacy embedded via Computing/PSHE/assemblies (critical thinking, deepfakes, verification).

Approved Tools & Product Safety

- Staff may only use AI tools that do not require personal/sensitive data OR, if such data is necessary, tools listed on the Approved AI Tools Register (Appendix K). New tools require **AI Tool Evaluation (Appendix D) + DPIA (Appendix E)** + IT Director & DPO sign-off.
- **DfE Product Safety expectations** (minimum): harmful content filtering, persistent moderation, activity logging & alerts, age-differentiated controls, clear privacy notices, IP protections (no retention for vendor model training without explicit consent). Record outcome in the Register.

Safeguarding, Filtering & Monitoring

- **Default controls:** Real-time supervision; AI transcripts/logs retained for safeguarding/audit per schedule; monitoring aligned to Online Safety Policy.
- **Primary (KS1–2):** Direct pupil use is exceptional, brief, fully supervised; emphasis on teacher-only use and early digital literacy.
- **Secondary (KS3–5):** Structured pupil use under teacher direction; parental consent where tool ToS require; Behaviour Policy covers misuse.
- **Incidents:** Any harmful/inappropriate AI output or misuse is reported to the DSL and recorded (CPOMS or local system). DSL leads response per KCSIE and Online Safety policy.

Staff Use — Professional Standards

Staff must:

- **Never paste personal data** (pupil, parent, staff) into public AI systems not approved on the Register.
- **Critically evaluate** AI outputs (accuracy, bias, age suitability); never provide unreviewed outputs to pupils.
- **Respect IP:** Don't upload copyrighted works without permission/exception; don't publish AI outputs externally without checks.
- **Assessment:** No high-stakes grading/placement solely by AI; teachers retain final judgment.
- **Follow AUP controls:** No personal email for Trust business/AI accounts are allowed; you must use an email address with an end suffix of either
 - bcwcat.co.uk
 - sbsj.co.uk
 - holyfamilyschool.uk
- Protect accounts (password rules, MFA) and devices; expect lawful monitoring on your AI account platforms.

Student Use — Pupil Code of Conduct (Summary)

Students must:

- Use AI only with permission and supervision; disclose AI assistance when required.
- Never use AI to cheat, impersonate, bully, or generate harmful content; consequences per Behaviour/Academic Integrity.
- Protect privacy (no personal details in prompts); report any concerning outputs to staff.
- Think critically: verify AI information, AI isn't always right.
(Full Code in Appendix C; complements pupil AUP.)

Academic Integrity & Assessment

- Design assessment to minimise AI misuse (in-class tasks, oracy, process evidence).
- Where AI is permitted and if instructed to do so by a tutor, students must complete the Student AI Declaration (Appendix F).
- Follow JCQ/Ofqual expectations: no automated high-stakes marking; proportionate malpractice investigation.

Data Protection & DPIAs

- **Default:** Avoid entering personal/sensitive data into GenAI.
- Where necessary, complete a DPIA and secure a compliant Data Processing Agreement (vendor). Address purposes, lawful basis, minimisation, storage location, retention, children's rights (AADC), transparency, model-training opt-outs, and security. Record in RoPA.
- **ADM:** BCWCAT will not make legally/significantly affecting decisions solely by AI. Provide human review on request and respect subject rights.

Security & Technical Standards

- **Identity & Access:** MFA for staff accounts where possible; student MFA per AUP (mandatory for secondary out-of-school access; advisory/exception-based in primary). Password rules per AUP.
- **Devices/BYOD:** Trust rules apply; encryption, secure email, no storing sensitive AI outputs locally on machines that are not the property of BCWCAT.
- **Filtering/Monitoring:** Age-appropriate filtering and monitoring in line with Online Safety Policy; logs retained and reviewed.
- **Records/Retention:** AI artefacts are scheduled under IRMS retention guidance (Appendix M).

Communications & Transparency

- **Privacy Notices:** Reference AI uses and associated rights with links to staff/pupil notices.

Incident Response & Reporting

- **Safeguarding incidents:** Report immediately to DSL; record actions/outcomes; contact external agencies as required.
- **Data breaches:** Follow Trust breach process; log within 72 hours and escalate to DPO who assesses ICO notification; maintain audit trail. (Use Appendix I).
- **FOI/Subject rights:** Requests handled via existing FOI/data rights processes.

Procurement & Contracts

- Complete AI Tool Evaluation (Appendix D) + DPIA (Appendix E) before deployment; require clear vendor DPA terms, sub-processor transparency, UK/adequate storage,

defined retention, and no vendor model-training on Trust data without explicit consent.
Add tool to Register with permitted uses and age bracket.

Governance, Assurance & Audit

- Annual review of the **AI Tools Register** and DPIAs;
- Publication scheme updates (policy and register).

Related Policies & Guidance (read alongside)

- Online Safety Policy (2025).
- Acceptable Use Policy (Staff, Governors, Contractors) (2025).
- Data Protection Policy (2025).
- Privacy Notices (Staff & Governors; Pupils & Families) (2025). [turn0file56?](#)
- Freedom of Information Policy & Published Guide to Information. [turn0file54?](#)
- Safeguarding & Lettings Addendum (KCSIE para 167).
- IRMS Academies Toolkit (records/retention).
- DfE Safe & Effective Use of AI — Leadership & Staff modules (June 2025). [turn0file47?](#)

Version Control

- v1.0 (September 2025): New policy for Board approval.

Appendix A — Glossary of AI Terms (plain English)

AI (Artificial Intelligence)

Software that can do tasks that usually need human intelligence, such as recognising patterns, understanding language, or making predictions.

Generative AI (GenAI)

AI that creates new content—text, images, audio, video, or code—when you ask it to.

Large Language Model (LLM)

A type of GenAI trained on lots of text so it can respond to prompts in natural language (e.g., chat assistants).

Prompt

The instructions or question you give to an AI tool. Good prompts are clear about task, audience, tone, and constraints.

System Prompt

The “hidden” or initial instructions that set the AI’s role and boundaries (e.g., safety rules). Users usually don’t see these.

Tokens

Small chunks of text that AI uses under the hood. Longer prompts/answers use more tokens (which may affect cost and limits).

Hallucination

When an AI confidently makes something up or gets facts wrong. Always check important outputs.

Bias

Systematic unfairness in data or outputs (e.g., stereotypes). We reduce bias by careful design, review, and inclusive examples.

Prompt Injection

A malicious or unintended instruction inside content (or links/files) that tries to override the AI’s rules. Treat unknown inputs cautiously.

Data Poisoning

When training or reference data is tampered with to mislead the model or skew results.

Model Training

Teaching an AI model patterns from data. Can be:

- **Pre-training:** Learning general language/patterns from large datasets.
- **Fine-tuning:** Additional training on smaller, task-specific data (e.g., curriculum-aligned marking rubrics).

RAG (Retrieval-Augmented Generation)

An approach where the AI fetches trusted documents first, then uses them to answer—reducing hallucinations and improving accuracy.

Few-shot / Zero-shot

Giving a model a few examples in the prompt (few-shot) or none (zero-shot) to show the pattern you want.

Agent

An AI that can plan steps and use tools (e.g., browse, calculate) to complete a task. Keep strong safeguards and human oversight.

Automated Decision-Making (ADM)

Decisions about a person made by technology with little or no human input. Under GDPR, legally or significantly affecting decisions must not be made solely by AI—meaningful human review is required.

Human-in-the-Loop (HITL)

A trained adult (e.g., teacher) reviews, edits, and takes responsibility for AI outputs before action is taken or content is given to pupils.

Safety / Moderation

Filters and policies that block harmful or inappropriate content (e.g., self-harm, hate). In schools, logs and alerts support safeguarding.

Age Gating / Age-Appropriate Design

Controls that match features/permissions to a pupil's age and maturity (linked to the ICO Children's Code).

Data Minimisation

Only collect/use the least personal data necessary for the task. Avoid entering names or sensitive details unless essential and approved.

Personal Data / Special Category Data

Information that identifies someone (personal data). Extra-sensitive data (health, ethnicity, religion, etc.) is "special category" and needs stronger protection.

Pseudonymisation / Anonymisation

- **Pseudonymisation:** Replace names with codes but keep a key separately.
- **Anonymisation:** Remove identifiers so no one can be identified.

Lawful Basis

The legal reason for processing personal data (e.g., public task, legitimate interests, consent). Must be identified before use.

DPIA (Data Protection Impact Assessment)

A risk assessment required when processing could be high-risk (e.g., using AI with pupil data). It documents risks and the controls to reduce them.

DPA (Data Processing Agreement)

A contract with a vendor that sets out how they'll protect and use our data (storage, security, retention, training opt-outs, subprocessors).

Transparency / Disclosure

Being open about when and how AI was used (e.g., staff note "assisted by AI," pupils complete a declaration where required).

Intellectual Property (IP) & Copyright

Rights that protect creators' work. Don't upload or share copyrighted content without permission or a clear exception; review AI outputs before publishing.

Accessibility

Features that help everyone participate (e.g., text-to-speech, reading level simplification). Use tools that support SEND and inclusion.

Academic Integrity

Honest work. Using AI to think with is different from using it to do the work for you. Follow task rules and declare permitted AI help.

Marking / Feedback Automation

AI can draft feedback or help with low-stakes marking, but teachers stay in charge of judgements—no high-stakes decisions by AI alone.

Red Teaming / Safety Testing

Deliberate testing to find failures (e.g., harmful outputs, leaks) so controls can be improved.

Watermarking / Detection

Techniques that label or help detect AI-generated media. Helpful but not foolproof—always use professional judgement.

Deepfake

Synthetic media that convincingly impersonates a person. Treat unexpected or sensational content sceptically; report concerns.

Audit Log

A record of who used an AI tool, when, and for what. Supports safeguarding, security, and compliance checks.

Retention

How long data or chat logs are kept before secure deletion. Must follow our retention schedule.

Approved Tools Register

The Trust list of AI tools vetted for safety, privacy, and suitability. If it's not on the list (or explicitly approved), don't use it with personal data.

Incident

Any harmful output, misuse, or data/privacy concern. Report immediately to the DSL (for safeguarding) and/or DPO (for data protection).

Acceptable Use

The do's and don'ts for staff and pupils when using AI and technology—aligned with safeguarding and behaviour policies.

Filtering & Monitoring

Technical controls that block and flag risky content or behaviour, with appropriate oversight and proportionate response.

Vendor / Sub-processor

The company providing the tool (vendor) and any other companies they use to process data (sub-processors). Must be listed and contractually controlled.

Opt-Out from Model Training

A guarantee that our inputs/outputs aren't reused to train the vendor's commercial models unless we explicitly agree (and, for children, have parental consent where needed).

— End of Appendix A —

Appendix B — Roles & Key Contacts

- **Trust AI Lead (IT Director):** Mr Christopher Jakubowski chris.jakubowski@bcwcat.co.uk
- **DPO:** Mr Richard Lewis-Ogden (Bywater Kent) richard@bywaterkent.co.uk
- **DSL:** Mrs Anna Gautrey anna.gautrey@bcwcat.co.uk
- **IT Helpdesk:** support@bcwcat.co.uk

Appendix C — Pupil AI Code of Conduct (Primary & Secondary)

Primary (KS1–2)

- I will only use AI when my teacher says so and with an adult watching.
- I will never share personal information (name, address, phone, school).
- If I see something that makes me uncomfortable, I will tell an adult.

Secondary (KS3–5)

- I will only use AI when allowed by my teacher and I will declare AI help in my work.
- I will not use AI to cheat, impersonate, bully or create harmful content.
- I will protect my privacy (no personal details in prompts) and report concerns promptly.
(Complementary to the Pupil Acceptable Use Agreement.)

Appendix D — AI Tool Evaluation Form (pre-DPIA triage)

Purpose & Pedagogy: Intended use case; benefits; safer alternatives considered.

User group: Staff / Pupils (age bracket).

Data in/out: Will personal or special category data be input? Y/N (if Y → DPIA).

Safety & Controls: Harm filtering; moderation; logging; age gates; teacher dashboards.

Compliance: Vendor privacy notice clarity; data location; retention; sub-processors; opt-out of model training; T&Cs on under-18s.

Technical: SSO/MFA; audit logs; API limits; content watermarking for deepfakes (if applicable).

Decision: Approved / Approved with conditions / Not approved.
(Leads into DPIA; aligns with DfE product safety expectations and AUP/security.)

Appendix E — DPIA Addendum for Generative AI

Add to your standard DPIA:

- **Lawful basis** (Art. 6) and **special category condition** (Art. 9) if any.
- **Children's Code** measures: high privacy defaults, clarity, data minimisation.
- **Risks:** Inappropriate outputs; hallucinations; bias; prompt injection; IP; ADM; re-identification; deepfakes.
- **Mitigations:** Age-gates; supervised use; pre-approved prompts; content filters; teacher review; opt-out from vendor training; local logging; staff training; student declarations.
- **Residual risk & sign-off:**

IT Director : _____

Date : _____

Appendix F — Student AI Declaration (for assignments)

Unit/Task : _____

Teacher : _____

Date : _____

Prompted AI used? Y/N (Tool: [_____])

What AI did: (e.g., drafted outline, transformed reading level)

What I did: (edits, fact-checks, sources used)

I confirm I have followed the Pupil AI Code and Academic Integrity policy.

Student signature: _____

(Helps teachers see process & compliance.)

Appendix G — Staff AI Use Addendum (attach to Staff AUP)

- Use **Trust accounts only** (no personal email/accounts).
- **No uploading** personal data unless the tool is approved and DPIA'd.
- Treat outputs as **draft**; verify accuracy/bias; cite sources; respect IP.
- Store any necessary logs/outputs in **approved locations** only; follow retention.
- **Report incidents** to DSL (safeguarding) and IT/DPO (data/security). [Turn0file53](#)

Appendix H — AI Prompt & Output Log (optional where required)

- **Class/Team:** [] **Tool:** [] **Date:** []
- **Purpose:** [lesson planning / resource adaptation / admin ...]
- **Prompts used (no personal data):** []
- **Output check:** (accuracy, bias, age-appropriateness) []
- **Storage location/retention:** [SharePoint path/date]
(Use only when pedagogically necessary; otherwise avoid collecting excess data.)

Appendix I — AI Incident Report (safeguarding/data/security)

Incident forms must be logged centrally with the DSL and DPO

- **Type:** [Harmful content exposure / Bullying / Impersonation / Data breach / Tech failure]
- **Who/When/Where:**
- **Tool:**
- **What happened:**
- **Immediate action:** [blocked content/tool; supported pupil; preserved evidence]
- **Escalation:** [DSL notified time/date; DPO if data involved]
- **Outcome/Follow-up:** [parent informed; sanctions; training; tech change]

Appendix K — Approved AI Tools Register (published summary)

Tool	Use case	Age	Personal data?	DPIA ref	DP terms (location/retention/training opt-out)	Status	Review
ChatGPT Team Edition	General AI prompting for administration and curriculum	Any	Yes, following GDPR best practises		Users must opt out of any data scraping of training.	Active	09/2026
TeachMateAI (All Editions)	For lesson planning and curriculum	Any	Yes, following GDPR best practises		Attend a TMAI workshop PPA session (Advisory).	Active	09/2026
Microsoft Co-Pilot (Paid Edition)	General AI prompting for administration and curriculum	Any	Yes, following GDPR best practises		Please note this refers to the licenced paid edition of Microsoft co-pilot, £25 per month per user, not to be confused with the free version of Co-pilot, if you are unsure, please ask the IT Director	Active	09/2026

For submissions to Appendix K you can email ai@bcwcat.co.uk.

Appendix L — Filtering & Monitoring Baseline for AI

- Classroom supervision; teacher dashboards switched on.
 - SafeSearch/AI safety modes; blocked categories per Online Safety Policy.
 - Staff and secondary students use **MFA** per AUP; logs retained per schedule; reviews by DSL/IT.
-

Appendix M — Retention Schedule (AI artefacts)

- **AI incident logs:** *Current + 6 years* (staff) / until pupil **DOB+25** (pupil cases).
 - **DPIAs, tool evaluations, contracts:** *Life of tool + 6 years*.
 - **Student AI declarations (assessment evidence):** Follow assessment/QA retention then dispose.
 - **Lesson/resource prompts/outputs:** Retain only if required for audit; otherwise delete. (Use IRMS Academies Toolkit principles and your DP Policy/retention scheme.)
-

Appendix N — Coursework & Exams Guidance

- Where boards disallow AI assistance, state this clearly and use **in-class process checks** (plans, drafts, orals).
 - Where limited assistance is allowed, require **Appendix F** and teacher commentary on authenticity. (Align with JCQ/Ofqual expectations noted in §11.)
-

Appendix O — Safe Lesson Patterns with AI (examples)

- **Reading-level adaptation (teacher-only):** Paste anonymised text, request age-appropriate summary; teacher checks; share to class.
- **Critical AI literacy:** Show AI output with deliberate errors/bias; pupils identify/fix with sources.
- **SEND support:** Teacher adapts instructions/visual schedules, no personal data, then checks for suitability.
- **Website transparency:** Ensure Privacy Notices (workforce & pupils/families) mention AI use where relevant.