CRESTWOOD
COMMUNITY SCHOOL

Acceptable Use of Artificial Intelligence Policy

July 2026
Review date: July 2027

Policy Purpose and Scope
Artificial Intelligence (AI) is an increasingly valuable tool within education. This policy aims to ensure that AI technologies are used safely, ethically and responsibly by all staff members. The primary objective is to harness the benefits of AI while robustly protecting students, staff, parents/carers, school data, confidential information and the school's professional reputation.
This policy applies to all employees, governors, contractors and visitors who utilise AI technologies for school purposes or on school-managed networks and devices.

Policy Statement
The school recognises that AI can be used to significantly improve teacher workload, increase productivity, support lesson planning, improve accessibility and assist with curriculum development and communication.

However, **AI must never replace professional human judgement.** All users remain fully and legally responsible for any content, decision, or resource produced or assisted by AI tools.

Guiding Principles
All staff members must ensure that their use of AI is consistently aligned with the following core principles -

- **Safety and Security -** protecting the digital and physical safety of the school community
- **Ethical and Transparent -** being open about when and how AI is utilised
- **Legal and GDPR Compliant -** ensuring absolute data privacy and adherence to UK data laws
- **Inclusive and Age Appropriate -** promoting equity and safeguarding younger audiences
- **Accurate -** rigorously verifying facts and outputs

Data Protection, GDPR and Confidentiality
Data protection is paramount. Staff must maintain a strict boundary between school data and AI platforms to prevent unlawful data processing.

Prohibited Data Inputs
Staff **must never** input personal or identifiable data into any AI platform other than when signed into the Crestwood Community School Gemini Workplace account. This includes, but is not limited to -

- **Identifiers -** names (staff, students, parents/carers), email addresses, phone numbers and home addresses
- **Sensitive Records -** medical information, Special Educational Needs and Disabilities (SEND) information, safeguarding records, CPOMS data, Child

Protection disclosures, behaviour records and attendance logs
- **Operational and HR Data -** HR documentation, performance management documents, payroll information, or individual assessment data that could identify a student.

Confidential School Information

You must only use the School's Gemini Workplace account to upload, process, or summarise confidential corporate or institutional information. You must not use any other AI tool. This includes -

- Internal investigations, HR cases, grievances or disciplinary documentation
- Confidential meeting minutes
- Financial documents, budgets and pre-publication examination papers
- Passwords, network configurations and security procedures

Approved AI Platforms and Ecosystem Expectations

To ensure school security settings remain active, audit logs exist and data is protected. Staff should primarily use AI tools already integrated into the School's managed network.

- *Google Workspace Expectations* - Where possible, staff should exclusively utilise AI features within the school's managed Google Workspace environment -
    - Google Classroom and Google Drive
    - Google docs, slides, sheets and forms
    - Google Meet
- *Approved Platforms List* - Staff are permitted to use the following approved platforms through their official school account -
    - Gemini (within Google workspace for education)
    - Google NotebookLM (where explicitly enabled by IT administration)
    - Canva Magic Studio (verified school account only)
    - Adobe Firefly (verified school account only)
    - *Note - Use of personal AI accounts for school work is strictly prohibited unless specifically authorised in writing by the Senior Leadership Team*

Framework for AI Usage
Acceptable Uses

AI may be used as a supportive assistant across the following areas:

Category	Permitted Use Cases
Teaching & Learning	Lesson planning, differentiation ideas, worksheet generation, quiz creation, model answers, success criteria, knowledge organizers, retrieval practice, homework tasks, and revision resources.
Administration	Drafting emails, parent communications, report templates, behavior letters, meeting agendas, risk assessment templates, policy drafting, and staff briefings.
Leadership & Strategy	Curriculum planning assistance, anonymized data interpretation, resource creation, action/improvement plans, department documentation, and CPD materials.
Accessibility	Simplifying complex reading materials, generating dyslexia-friendly text structures, translation, readability improvements, and formatting alternative layouts.

Unacceptable Uses

Staff **must never** use AI to automate critical professional duties or generate deceptive media. Prohibited uses include:

- **Critical Decision Making:** Making safeguarding decisions, determining disciplinary outcomes, or diagnosing SEND and mental health conditions.
- **Evidence & Accountability:** Writing witness statements, producing fabricated evidence, automatically grading coursework, or marking examinations without human review.
- **Automated Communication:** Contacting parents automatically via AI without strict human oversight and review.

- **Deceptive Media:** Creating artificial images of students/staff, cloning voices, generating deepfakes, or misrepresenting school communications.

🟢 Green – Appropriate	🟡 Amber – Use with Caution	🔴 Red – Not Permitted
Lesson planning	Drafting reports (must be checked)	Uploading student names
Quiz generation	Parent emails (must be reviewed)	Safeguarding records
Differentiated resources	Performance data summaries	HR investigations
Knowledge organisers	Assessment feedback (teacher-reviewed)	CPOMS content
Retrieval practice	Behaviour letters (teacher-reviewed)	Medical information
Display materials	Curriculum planning	Staff grievances
Revision resources	Policy drafting	Confidential meeting notes
Translation support	Data analysis (anonymised)	Passwords or security details
Accessibility support	Meeting summaries	Deepfakes or voice cloning

Quality Assurance and Risk Management

Human Oversight

AI should assist decision-making—never replace it. Every single AI-generated output must be heavily vetted by the user.

- ***The Review Process:*** Staff must check, edit, proofread, fact-check, and review every output for hidden bias before it is deployed or shared.

Accuracy

AI models are known to invent facts, misquote sources, produce outdated information and display systemic bias. Staff bear ultimate responsibility for verifying the accuracy of all information before utilising it in a professional capacity.

Copyright & Intellectual Property

Staff must ensure that AI-generated content does not breach copyright laws or unlawfully copy published educational resources. Content must be appropriately adapted and meet all standard licensing requirements.

Equality and Bias

AI systems train on broad internet data and can unintentionally replicate discriminatory biases. Staff must actively review outputs to ensure they are inclusive, fair, representative, free from discriminatory language, and appropriate for the intended school audience.

Roles and Responsibilities

Staff Responsibilities

- Complete mandatory school-provided AI awareness training.
- Adhere strictly to this policy and the overarching ICT Acceptable Use Policy.
- Protect confidential and personal data at all times.
- Utilise only approved, school-licensed AI tools.
- Report any system concerns, data inaccuracies, or policy misuse to the designated AI Lead, the Network Manager and/or SLT.
- Seek immediate advice from line management if unsure about the appropriateness of an AI tool.

Senior Leadership Responsibilities

- Maintain, update, and distribute the list of approved school AI platforms.
- Regularly review AI use and technological impacts across the school.
- Ensure technical configurations maintain strict GDPR compliance.
- Provide up-to-date staff training and monitor emerging technological risks.
- Review this policy annually, or sooner in the event of significant legislative changes.

Compliance, Monitoring and Reporting

Monitoring

The school reserves the right to monitor the use of school Google accounts, Google Workspace/Classroom activity, and approved AI platform usage. Monitoring is conducted to ensure compliance with this policy, in accordance with the school's *ICT Acceptable Use Policy*, *Data Protection Policy*, and relevant employment legislation.

Reporting Concerns

Any identified data breaches, AI misuse, unsafe content generation, inappropriate outputs, or safeguarding risks must be reported immediately to:

- The Headteacher or member of SLT
- The Designated Safeguarding Lead (DSL)

- The Data Protection Officer (DPO)
- Your Line Manager

Related Policies

This document must be read in conjunction with the following school policies:

- *Data Protection (GDPR) Policy*
- *ICT Acceptable Use Policy*
- *Safeguarding & Child Protection Policy*
- *Online Safety Policy*
- *Staff Code of Conduct*
- *Behaviour Policy*

School AI Champions -

Steve Topazio, Deputy Headteacher	s.topazio@crestwood.hants.sch.uk
Sam Clark, Network Manager	s.clark@crestwood.hants.sch.uk
Peter Willmore, IT Assistant	p.willmore@crestwood.hants.sch.uk
Jacob Moran, Teacher of IT	j.moran@crestwood.hants.sch.uk

Staff Declaration

When you have read this policy, please complete the googleform here to confirm that you have read and understood the policy.

Signed Headteacher:- ____ 

Print Name:- ___KRISTA DAWKINS_____

Signed Chair of Governors:- _____

Print Name:- _JOHN ANDERSON_____

Date:- July 2026

Review Date:- July 2027
(or when updates occur)