



**Harrison College Ltd**

## **Artificial Intelligence (AI) Policy**

Reviewed: January 2026  
Next review: January 2027

## Statement of Intent

Artificial Intelligence (AI) is a technology that can be used to create new content based on large volumes of data that models have been trained on from a variety of works and other sources. Generative AI is a rapidly evolving and increasingly freely available technology generating writing, audio, codes, images and video simulations. AI is the defining technology of our age, and it is evolving at incredible speed. This technology has the potential to benefit the economy and meet societal challenges. This is not new, and we already use AI in everyday life for email spam filtering, navigation apps and online chatbots.

While these technologies offer opportunities for teaching, learning and administration, they also introduce significant risks relating to data protection, safeguarding, academic integrity and misinformation. Worryingly, it can provide instructions for illegal or harmful activities.

Harrison College will consider the risks and challenges alongside the opportunities and benefits it brings. To ensure Harrison College creates a safe setting for using AI and reducing the risks associated with its use, we authorise the use of Microsoft Copilot only.

In allowing the use of AI at Harrison College, we will take care to follow our legal responsibilities in relation to the duty of care for our young people and staff, including those related to Data Protection, KCSIE and intellectual property law.

## Legal and compliance

Online safety should form a fundamental part of colleges' safeguarding and child protection measures. By taking a whole college approach to online safety, we aim to help make sure all staff, students, volunteers, mentors, business colleagues and parents know how they can help keep our young people safe online. Artificial Intelligence (AI) and the use of AI in college firmly sits within our policies and procedures governing our safe practice and compliance.

Government guidance across the UK including Working Together to Safeguard Children (2023) [Working together to safeguard children - GOV.UK](#) and Keeping Children Safe in Education legislation [Keeping children safe in education 2025](#) (annually updated) highlights the importance of safeguarding children and young people online, including Harrison College's responsibility to ensure our online procedures are safe as well as advising and supporting students and other users how to stay safe.

KCSIE sets out the legal duties to safeguard and promote the welfare of children and young people under the age of 18 in colleges, specifically

1. being aware of content risks under online safety, including disinformation, misinformation and conspiracy theories, and preventing access to harmful content
  - a. [Keeping children safe in education 2025](#)
  - b. Part one; what college staff need to know (11)
  - c. Part two; management of safeguarding
2. awareness of the DfE guidance on generative artificial intelligence (AI)
  - a. [Generative AI: product safety expectations - GOV.UK](#)
3. filtering and monitoring requirements placed on colleges to include training of staff and adhering to Cyber security standards

- a. [Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK](#)

The safeguarding duty of colleges is further set out in section 175 of the [Education Act 2002](#), the [Education \(Independent School Standards\) Regulations 2014](#), the [Non-Maintained Special Schools \(England\) Regulations 2015](#) and the [Apprenticeships, Skills, Children and Learning Act 2009](#).

Harrison College accepts accountability for safeguarding our young people. Due to the rapid development of AI technologies, Harrison College reserves the right to update this policy outside the normal review cycle where necessary to maintain safety, compliance, and best practice.

More information and detail on how we monitor and carry out our duties are included in our published policies found on our website. Please see here for more guidance [Statutory Information - Harrison College](#)

## **Artificial Intelligence Policy**

Safety will not be compromised. By adhering to this policy, we aim to foster a responsible and inclusive environment for the use of AI in education upholding privacy, fairness and transparency for the benefit of all involved. Therefore, we are implementing this policy so that the use of AI at Harrison College will prioritise safeguarding, data protection compliance and the wellbeing of staff and students. This policy should be used alongside our other child protection, online safety and safeguarding related policies and procedures.

The DfE have produced a guidance paper on AI which can be accessed here [Generative artificial intelligence \(AI\) in education - GOV.UK](#) and further information on security has been provided through the National Cyber Security Centre [ChatGPT and LLMs: what's the risk - NCSC.GOV.UK](#)

## **Authorised AI tools**

For the purposes of this policy, “authorised AI” refers to tools that have been formally approved by Harrison College following a Data Protection Impact Assessment (\*DPIA), technical security review and sign-off by the Principal Gemma Peebles (Data Protection Officer DPO) or delegated online safety lead (Gail Stonier). These tools and products provided or procured by Harrison College are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.

Other AI tools, which may be available for free or on a subscription basis and directly accessed by users via the internet are not authorised and must not be used. College information, student work or internal data may not be entered into such tools. These rules apply when using both Harrison College owned devices and any personal devices which may be used for work or internship purposes. No other AI tools may be used.

## **Users**

This policy applies the term “user” to all staff members employed at Harrison College whether as a consultant, contractor, on supply, trainees, temporary, or on service level agreements. It applies to all students who must also follow the policy and the acceptable use of IT policy. This also includes all stakeholders such as business and employers, volunteers and mentors carrying out college related sessions and using our systems or technology. We will be transparent and accountable about the use of AI technology so that all stakeholders, including staff, students, parents and other partners understand where and how AI is used and who is responsible.

## **Breaches**

The breach will be dealt with in line with Harrison College's IT Security and Acceptable Use Policy.

Breaches may include, but are not limited to, using unauthorised AI tools, entering personal data into AI systems, or relying on AI-generated output without appropriate professional oversight.

AI must never be used to make, influence or automate decisions relating to safeguarding, student behaviour, SEND provision, disciplinary action, recruitment or employment matters.

AI notetakers must not be used in safeguarding meetings, HR meetings, performance review discussions, medical meetings, or confidential student or staff meetings.

AI notetakers will never be used in a meeting without completing making all participants aware before the meeting starts. At meetings organised by Harrison College, our staff will let attendees know upfront that they should not use AI notetakers and as the meeting organiser our staff will take responsibility for the taking and distribution of notes.

Staff must report any concerns, inappropriate content or suspected misuse to the Principal or Designated safeguarding lead without delay.

All users should ensure that any suspected or confirmed security incidents are reported to the Data Protection Officer

All AI-generated content created for college purposes must be stored exclusively within college-approved systems. Staff must not download, transfer, or save AI-generated material to any personal devices, third-party platforms, or unapproved storage locations. This ensures compliance with our data protection, security, and governance requirements.

The Designated safeguarding lead will work collaboratively with our IT technology provider (Affinity IT) to ensure all filtering, monitoring and firewalls are in place to ensure safe internet use. This will include reviewing AI access logs and usage data periodically to identify unusual or risky behaviour. This partnership agreement includes termly review periods where alongside collaboration with the Directors, ongoing and future risks will be reviewed, risk assessments and DPIA's updated where applicable and the agreed use of AI tools and resources will be communicated to staff, students and other users.

The DPO, DSL and nominated leadership staff will have access to SENSO cloud based monitoring system and be able to identify unusual or risky behaviour. Incidents are recorded on this system and escalated and dealt with as necessary.

## **Training and support**

Harrison College sets out to offer guidance and establish a responsible and consistent approach to AI across our setting and users by fostering a culture of responsible AI use. We will educate staff and students about safe, responsible, ethical and legal use of AI. This will be achieved through various ways

- Implementing rigorous cybersecurity protocols and access controls through measures such as encryption, security patches and updates, access controls and secure storage

- Engaging students in conversations about data protection, privacy, bias, safeguarding, and the social impact of AI applications.
- Incorporating AI education into the curriculum to provide students with an understanding of AI's capabilities, limitations, and ethical implications.
- Providing guidance on identifying reliable and trustworthy AI sources and evaluating the credibility and accuracy of AI-generated information.
- Briefings will be given on online safety and the use of AI-generated materials and use.
- Ensuring policies and procedures are accessible, referred to and made applicable to the various contexts they may be working in i.e. college sessions, internship opportunities, external business projects and emails and communication methods.
- Stipulating to staff during induction and annual updates that specific policies must be read and understood as part of their professional conduct and job descriptions.
- Staff will make themselves aware of and be accountable for informing students about the data collection, storage, and usage practices associated with AI technologies within their educational provision.
- Explaining the potential misuse of AI by those seeking to deceive, abuse or trick students into actions that they would otherwise not contemplate, for example interaction with others who are not who they claim to be but who can imitate who they claim to be using AI technology.
- Maintaining vigilance against material that may be deepfake or committing cyber fraud
- Ensuring users are aware of the controls and methods the college has put in place to manage the safe use of AI.
- To be aware of the intellectual property (IP) implications and copyright law.
- Incorporate AI as a teaching and learning tool to develop staff and students' AI literacy and skills
  - Staff and leaders must use their professional judgement when using these tools
  - Any content produced requires critical judgement to check for appropriateness and accuracy
  - The quality and content of any final documents remain the responsibility of the professional who produced it

Staff will receive appropriate training and support to effectively integrate authorised AI into their work including professional development opportunities focused on authorised AI tools and their effective integration into college administrative and teaching practices.

Training and support will be planned as part of staff personal development reviews and appraisals or on an as-needed basis. Staff have a responsibility to identify any training, and development needs to ensure they adhere to this policy and will discuss these with their line manager or senior leadership.

Free support materials for staff, developed by the Chiltern Learning Trust (CLT) and Chartered College of Teaching (CCT), to support the safe and effective use of generative AI in education can be accessed [Using AI in education settings: support materials - GOV.UK](#) and [Safe and effective use of AI in education - Chartered College of Teaching](#)

Staff who complete the training offered by CLT and CCT (endorsed by the DfE) can choose to complete the certified assessment to evidence their understanding of AI in practice.

## **Generative AI**

Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources. ChatGPT, Microsoft Copilot and Google

Gemini are generative AI tools, built on large language models (LLMs). LLMs are a category of foundation models trained on large amounts of data, enabling them to understand and generate human-like content. Tools such as ChatGPT, Microsoft Copilot and Google Gemini can answer questions, complete written tasks, generate images, text or code and respond to prompts in a human-like way. Other forms of generative AI can produce audio, simulations and videos

Advances in technology mean that we can now use these tools to produce AI-generated content. This creates opportunities and challenges for the college.

### **Challenges and risks**

The content produced by generative AI could be inaccurate, inappropriate or unsafe, biased, taken out of context, taken without permission (intellectual property infringement), out of date or unreliable or low quality. This is because generative AI returns results based on its training dataset, which may not be specific to our curriculum or setting. Therefore we do not authorise the use of public AI and LLM's and only authorise tools that are part of Harrison College's IT filtering and monitoring safeguard protection procedures. This ensures that our organisational data and personal information is not at risk.

**To ensure Harrison College creates a safe setting for using AI and reducing the risks associated with it's use, we authorise the use of Microsoft Copilot only.**

Users are expected to comply with the policy to ensure that AI tools are used appropriately.

### **Staff can use**

Authorised AI tools can assist staff in gathering and creating relevant educational resources, creating whole group or personalised lesson plans, generating extension tasks or scaffolded work, and identifying potential knowledge gaps. For instance, authorised AI platforms can suggest specific topics or learning activities. Teaching staff are permitted to use these suggestions as a starting point, incorporating their professional expertise to customise the lesson plans and make necessary adjustments to ensure individual student learning objectives are met. When staff use AI as part of their work, they will be clear where it has been used and what additional professional review or revision has been carried out.

Authorised AI tools can be utilised to automate certain aspects of marking of student work, such as multiple-choice or fill-in-the-blank surveys and questionnaires. Staff can use authorised AI-powered marking software to speed up scoring fact-based responses to objective questions, providing more time to support students individually. Staff must review outcomes to ensure accuracy and suitability.

Staff can also support students to gain feedback on their work themselves using authorised AI, replicating peer assessment processes. This will allow students to receive instant personalised and valuable feedback and improvement strategies on their work, helping to identify misconceptions and gaps in knowledge, as well as helping them develop more structured or creative writing. It is important that teaching staff play an integral role in this process and continue to monitor the feedback provided.

Staff can use authorised AI to assist in writing student reports (without sharing names or other personal data), ensuring accuracy and efficiency while maintaining their professional judgment. Where AI has been used to support with report writing, the staff member will always review and modify the AI-generated reports to ensure they reflect their own observations, assessments, and personalised feedback.

Staff will not use school AI tools or data for personal gain or for any means in contravention of applicable laws. Staff must not use AI to create harmful, deceptive or abusive content, including deepfake images or audio of staff or students. Any such behaviour will be treated as a serious safeguarding and disciplinary matter under the college Disciplinary policy

### **Students use**

As part of child protection and safeguarding policies and processes, the college will ensure that its students will continue to be protected from harmful content online, including that which may be produced by AI technology and that any authorised AI tools are assessed for appropriateness for individual students' age and educational needs.

Where deemed appropriate by staff, students will be permitted to explore and experiment with authorised, age-appropriate AI-based projects, allowing them to learn how to use AI for knowledge building, problem-solving, data analysis, and creative expression.

Students will be taught not to enter personal, sensitive or confidential data into Generative AI tools including their names, email and home addresses, date of birth etc.

Students must not upload their personal images, lesson materials or any internal college data content into any unauthorised AI system. This applies to any other students or staffs' images or personal information.

Students must not use AI to create harmful, deceptive or abusive content, including deepfake images or audio of staff or peers. Any such behaviour will be treated as a serious safeguarding and disciplinary matter

Students must not use unauthorised or consumer AI tools for any college-related purpose, including work on internships or project research.

### **Data Privacy**

It is important that users are aware of the data privacy implications when using generative AI tools. Staff and students must be aware that any information entered into a Generative AI model is no longer private, controllable or secure.

Personal data must be protected in accordance with data protection legislation.

Staff and students will not enter any personal information (personal data, intellectual property or private information (including commercially sensitive information, such as contracts) into any Generative AI model.

Harrison college will ensure that all steps are taken to protect the data and that the products and procedures comply with data protection legislation and our data privacy policy.

### **DPIA – Data Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) becomes necessary within this policy when the planned use of AI is likely to create a "high risk" to individuals' rights and freedoms. This is a requirement under the UK GDPR and recommended by the ICO. Carrying out a DPIA helps the college directors ensure a governance structure is in

place that is compliant with law and continually reviews the safety within a timely manner. By carrying out a DPIA, the college aims to identify and mitigate against potential issues early.

Assessment of the data protection aspects of the use of AI will include:

- The nature, scope, context and purposes of any processing of personal data and whether individuals are likely to expect such processing activities.
- What alternatives (both AI and non-AI) are there to the planned processing and what justification is there in choosing this method and how it is fair.
- A clear indication where AI processing and automated decisions may produce effects on individuals.
- Consideration of both individual and allocative harms (for example, selecting groups of students for different interventions results in gender or racial bias).
- How the use of the AI tool is proportionate and fair by assessing the benefits against the risks to the rights and freedoms to individuals and/or whether it is possible to put safeguards in place.
- When implementing new tools or technologies into the college environment.
- The potential impact of any security threats.
- A consideration of the rights and freedoms of individuals generally, not just in a data protection context, such as rights under the Equality Act 2010.

AI-generated content must be stored only on approved College systems and must not be retained longer than necessary. These permitted systems include;

SENSO

XELLO

SIMS

CPOM's

Global Bridge

Microsoft 365