

Use of Artificial Intelligence (AI) Policy

Reviewed:	March 2026
Review date:	March 2027
Person responsible for policy:	Director of Information & Systems
Publication:	Website
Overlaps with other policies:	Highlighted in turquoise

Contents

1. Aims and scope
2. Legislation and guidance
3. Regulatory principles
4. Roles and responsibilities
5. Staff and governors' use of AI
6. Educating pupils about AI
7. Use of AI by pupils
8. Formal assessments and academic integrity
9. Safeguarding and online safety
10. Cybersecurity
11. Staff training
12. Breach of this policy
13. Monitoring, transparency and review
14. Links with other policies

1. Aims and Scope

Here at Droitwich Spa High School and Sixth Form Centre we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. AI is rapidly becoming an integral part of education, influencing teaching methods, innovative administrative processes, and student learning. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding concerns, cybersecurity threats, and compliance with wider legal obligations.

Students are naturally exposed to and exploring the use of AI outside of the school environment and it is important that they are aware of the dangers and the safe and ethical use of AI.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole school community.

This policy covers the use of AI tools by school staff, governors, pupils and all third-party providers who use AI in the school environment. This includes generative chatbots such as ChatGPT and Google Gemini (please note, this list is not exhaustive).

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff to explore AI solutions to improve efficiency and reduce workload
- Prepare staff, governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff, governors, pupils and third-party providers
- Protect the privacy and personal data of staff, governors and pupils in compliance with the UK GDPR
- Ensure compliance with safeguarding, data protection, and academic integrity principles

1.1 Definitions

This policy refers to both 'open' and 'closed' generative AI tools. These are defined as follows:

- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information.
- **Closed generative AI tools** are generally more secure, as external parties cannot access the data you input.

2. Legislation and Guidance

This policy reflects good practice guidelines and recommendations in the following publications:

- AI regulation white paper, published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- Generative artificial intelligence (AI) and data protection in schools, published by the Department for Education (DfE)
- Keeping Children Safe in Education (KCSIE), published by the DfE
- DfE Guidance on Generative AI in Education 2025
- Joint Council for Qualifications (JCQ) AI in Assessments 2024

This policy also meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)

Source references:

Source	Title	Link
DfE	KCSIE	https://www.gov.uk/government/publications/keeping-children-safe-in-education
Legislature	UK GDPR and DPA 2018	https://www.legislation.gov.uk/ukpga/2018/12/contents
DfE	Guidance on Generative AI in Education 2025	https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education
JCQ	AI in Assessments 2024	https://www.jcq.org.uk/exams-office/malpractice/artificial-intelligence/
DfE	AI regulation white paper	Department for Science, Innovation and Technology, and the Office for Artificial Intelligence

3. Regulatory Principles

We follow the 5 principles set out in the AI regulation white paper.

Regulatory principle	WE WILL ...
Safety, security and robustness	<p>Ensure that AI solutions are secure and safe for users and protect users' data</p> <p>Ensure we can identify and rectify bias or error</p>

	<p>Anticipate threats such as hacking, phishing and cybersecurity vulnerabilities</p> <p>Monitor AI-related phishing scams, fraud, and cybersecurity risks</p>
Appropriate transparency and explainability	<p>Be transparent about our use of AI, and make sure we understand the suggestions it makes</p> <p>Ensure AI-generated content is identified where used</p> <p>Document the use of AI in assessment, recruitment, or administrative decision-making</p>
Fairness	<p>Only use AI solutions that are ethically appropriate, equitable and free from prejudice -- in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate</p> <p>Vet AI tools to ensure fairness and prevent bias</p> <p>Provide training to recognise AI bias and hallucinations and mitigate their impact</p>
Accountability and governance	<p>Ensure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI</p> <p>Ensure AI is not used to make independent decisions affecting students or staff</p> <p>Require human oversight for all AI output</p> <p>Hold all stakeholders responsible for any output shared that has been generated by AI</p>
Contestability and redress	<p>Make sure that staff are empowered to correct and overrule AI suggestions -- decisions should be made by the user of AI, not the technology</p> <p>Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment</p>

4. Roles and Responsibilities

Effective oversight and accountability are essential to ensure AI is used appropriately and safely within the school. The following sections define the key responsibilities of school leadership, staff, students, and IT teams in managing AI systems.

4.1 AI Lead

Our interim AI lead will be the Director of Information and Systems. They are responsible for the day-to-day leadership, ownership and management of AI use in the school.

The AI lead will work closely with the Director of Information & Systems, the DPO, and the DSL to ensure AI use aligns with school policies and national regulations.

4.2 Governing Board

The governing board will:

- Take overall responsibility for monitoring this policy and holding the Co-Headteachers to account for its implementation in line with the school's AI strategy
- Ensure the Co-Headteachers and AI lead are appropriately supported to make informed decisions regarding the effective and ethical use of AI in the school
- Ensure AI governance aligns with DfE, KCSIE, and GDPR regulations
- Adhere to the following guidelines to protect data when using generative AI tools:
 - Use only approved AI tools
 - Seek advice from the Director of Information & Systems, data protection officer, AI lead and the designated safeguarding lead, as appropriate
 - Check whether they are using an open or closed generative AI tool
 - Ensure there is no identifiable information included in what they put into open generative AI tools
 - Acknowledge or reference the use of generative AI in their work
 - Fact-check results to make sure the information is accurate
- Engage in annual update training to ensure compliance and risk mitigation for emerging risks

4.3 Co-Headteachers

The Co-Headteachers will:

- Liaise with the Director of Information & Systems and data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation
- Liaise with the DSL to ensure that the use of AI is in accordance with Keeping Children Safe in Education and the school's child protection and safeguarding policy
- Ensure that the guidance set out in this policy is followed by all staff
- Review and update this AI policy as appropriate, and at least annually (in February)
- Ensure staff are appropriately trained in the effective use and potential risks of AI
- Make sure pupils are taught about the effective use and potential risks of AI
- Sign off on approved uses of AI, or new AI tools, taking into account advice from the Director of Information & Systems, DPO, AI lead, and data protection impact assessments
- Conduct annual AI risk assessments and policy reviews
- Ensure AI use is transparent, fair, and free from bias
- Engage in annual update training to ensure compliance and risk mitigation for emerging risks

4.4 Director of Information & Systems

The Director of Information & Systems is responsible for:

- Implementing security measures to ensure AI tools comply with data protection laws
- Ensuring that AI tools used in school settings do not process or store personal data without anonymisation
- Ensuring that all technologies undertake a minimum annual Data Protection Impact Assessment (DPIA) before use is permitted within Droitwich Spa High School and Sixth Form Centre
- Conducting regular cybersecurity audits to monitor AI-related risks
- Ensuring AI tools do not introduce security vulnerabilities
- Working with the DPO and AI lead to approve new AI tools
- Engaging in annual update training to ensure compliance and risk mitigation for emerging risks

4.5 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI. Our DPO is contactable via privacy@droitwichspahigh.worcs.sch.uk.

The DPO will:

- Advise on data protection compliance for all AI tools
- Conduct Data Protection Impact Assessments (DPIAs) before new AI tools are introduced
- Work with the Director of Information & Systems to ensure AI tools comply with UK GDPR and DPA 2018

4.6 Designated Safeguarding Lead (DSL)

The DSL is responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:

- Being aware of new and emerging safeguarding threats posed by AI, including:
 - AI-generated deepfakes
 - Misinformation and disinformation
 - Impersonation risks
 - Sexual grooming
 - Sexual harassment
 - Sexual extortion
 - Child sexual abuse/exploitation material
 - Harmful content
 - Harmful advertisements and promotions
 - Bullying
- Updating and delivering staff training on AI safeguarding threats
- Responding to safeguarding incidents in line with Keeping Children Safe in Education (KCSIE) and the school's child protection and safeguarding policy

- Understanding the filtering and monitoring systems and processes in place on school devices, ensuring they comply with the Government's Filtering and Monitoring Standards
- Ensuring the school's filtering and monitoring systems detect and prevent AI-generated threats

The school's DSL is **Jamie Broughton** and is contactable via email, BroughtonJD@droitwichspahigh.worcs.sch.uk.

4.7 Teaching and Support Staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy.

Teachers and professional services staff are responsible for ensuring AI is used as an educational aid while maintaining academic integrity, supporting student learning, and preventing misuse.

Responsibilities:

- Use AI as a teaching aid, not as a replacement for pedagogy
- Verify AI-generated content for accuracy, appropriateness, and bias
- Educate students on AI literacy, misinformation, and deepfakes
- Ensure AI use does not compromise academic integrity or safeguarding
- Monitor for sudden changes in student work that suggest AI misuse; work that is suddenly better than previously seen, Americanisation or other hallmarks of AI-generated content
- Engage in annual update training to ensure compliance and risk mitigation for emerging risks

To protect data when using generative AI tools, staff must:

- Use only approved AI tools (see section 5)
- Seek advice from the Director of Information & Systems, data protection officer, or AI lead, as appropriate
- Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy
- Check whether they are using an open or closed generative AI tool
- Ensure there is no identifiable information included in what they put into open generative AI tools
- Ensure AI inputs are anonymised where possible, and if that is not possible, seek approval from the IT and Data Protection team
- **NOT use any new software without prior permission from the IT and Data Protection team**
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

4.8 Pupils

Students must develop an understanding of AI's capabilities and limitations while using AI tools ethically and responsibly within the guidelines set by the school.

Pupils must:

- Follow the guidelines set out in section 7 of this policy ('Use of AI by pupils')
- Use AI tools responsibly and in line with school policies
- Declare AI use in coursework, assignments, and assessments where required
- Understand ethical considerations and avoid over-reliance on AI

5. Staff and Governors' Use of AI

5.1 Approved Use of AI

We are committed to helping staff and governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff or governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the school has approved its use does not mean it will always be appropriate.

5.2 Process for Approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. Staff should contact the Co-Headteachers to discuss any ideas they may have with regards to using AI, so the Co-Headteachers can take the suggestions forward if they deem it to be a satisfactory new method of working.

The Co-Headteachers is responsible for signing off on approved uses of AI, or new AI tools, taking into account advice from:

- The AI lead
- The Director of Information & Systems
- The DPO

- Data protection impact assessments (DPIAs)

Before any new AI tools are introduced:

- A Data Protection Impact Assessment (DPIA) must be conducted by the DPO and Director of Information & Systems
- All technologies must undertake a minimum annual DPIA before continued use is permitted
- **Staff are NOT permitted to use any new software without prior permission from the IT and Data Protection team**

5.3 Data Protection and Privacy

To comply with data protection regulations, AI tools must not process personal data unless explicitly approved. Where possible, anonymisation techniques should be used to protect individual privacy.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

Key requirements:

- AI tools must not process or store personally identifiable student or staff data unless explicitly approved by the Director of Information & Systems and Data Protection team
- AI inputs should be anonymised where possible, and if that is not possible, approval must be sought from the IT and Data Protection team
- A Data Protection Impact Assessment (DPIA) must be conducted before any new AI tools are introduced
- **Staff are NOT permitted to use any new software without prior permission from the IT and Data Protection team**

If personal and/or sensitive data is entered into any generative AI tool, other than Co-Pilot, Droitwich Spa High School and Sixth Form Centre will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

Please also refer to section 12 of this policy.

5.4 Intellectual Property

Most generative AI tools use inputs submitted by users to train and refine their models.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.

Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited -- we will seek legal advice if we are unsure as to whether we are acting within the law.

5.5 Bias and Fairness

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output.

AI systems must be reviewed and monitored to minimise bias, ensuring fairness in learning, assessment, and administrative decision making.

We will:

- Vet AI tools to ensure fairness and prevent bias
- Provide training to recognise AI bias and hallucinations and mitigate their impact
- Require human checking for all AI output
- Hold all stakeholders responsible for any output shared that has been generated by AI
- Ensure we can identify and rectify bias or error by training staff in this area
- Regularly review our use of AI to identify and correct any biases that may arise

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

5.6 Transparency and Accountability

It is essential that AI use within the school remains transparent, and that decisions made using AI are documented and subject to human oversight.

- AI must not be used to make independent decisions affecting students or staff
- The use of AI in assessment, recruitment, or administrative decision-making must be documented
- AI-generated content must be identified where used
- Human oversight is required for all AI output
- All stakeholders are responsible for any output shared that has been generated by AI

5.7 Raising Concerns

We encourage staff and governors to speak to the Co-Headteachers in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

Safeguarding concerns arising from the use of generative AI must be reported immediately to the DSL in accordance with our school's child protection and safeguarding policy.

5.8 Ethical and Responsible Use

We will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our school's equality policy when using generative AI tools.
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff and governors must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt
- Use AI tools to create harmful, misleading, or inappropriate content

6. Educating Pupils About AI

Here at Droitwich Spa High School and Sixth Form Centre we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI.

Pupils are taught in our curriculum about:

- The potential benefits of using AI tools to aid their learning
- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How to recognise AI bias and hallucinations
- AI-generated deepfakes, misinformation, and impersonation risks
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content
- Ethical considerations when using AI
- How to avoid over-reliance on AI

7. Use of AI by Pupils

We recognise that AI has many uses to help pupils learn.

7.1 Acceptable Use

Pupils may use AI tools:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

7.2 Prohibited Use

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments, including internal and external assessments, and coursework (unless specifically permitted and declared -- see section 8)
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)
- To generate coursework, essays or exam content without declaration

This list of AI misuse is not exhaustive.

7.3 Referencing and Attribution

Where AI tools have been used as a source of information, pupils must reference their use of AI. The reference must show:

- The name of the AI source
- The date the content was generated

We consider any unattributed use of AI-generated text or imagery to be plagiarism and will follow our plagiarism procedures.

7.4 Ethical Use by Pupils

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person
- Generate or share explicit or offensive content, including, but not limited to, generating inappropriate or sexualised images of pupils
- Input offensive, discriminatory or inappropriate content as a prompt
- Use AI tools to create harmful, misleading, or inappropriate content

8. Formal Assessments and Academic Integrity

AI must not compromise academic integrity. This section ensures that students and staff adhere to fair assessment practices while using AI tools appropriately.

8.1 Preventing AI Misuse in Assessments

To maintain assessment integrity, students must declare AI-assisted work, and staff must monitor submissions for signs of unauthorised AI use.

Key requirements:

- AI must not be used to generate coursework, essays or exam content unless specifically permitted and declared
- Students must declare any AI-assisted work in line with JCQ and school regulations
- Staff must monitor for sudden changes in student work that suggest AI misuse, including:
 - Work that is suddenly better than previously seen
 - Americanisation of spelling or language
 - Other hallmarks of AI-generated content
 - Unusual phrasing or vocabulary inconsistent with the student's previous work

8.2 JCQ Compliance

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.

We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on AI use in assessments.

9. Safeguarding and Online Safety

AI must be used safely within the school environment, preventing harm and ensuring students and staff understand the potential risks associated with AI-generated content.

9.1 AI-Related Safeguarding Risks

The school is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- **AI-generated deepfakes** -- realistic but fake images, videos or audio
- **Misinformation and disinformation** -- false or misleading information
- **Impersonation risks** -- AI being used to impersonate students, staff or others
- **Sexual grooming**
- **Sexual harassment**
- **Sexual extortion**
- **Child sexual abuse/exploitation material**
- **Harmful content**
- **Harmful advertisements and promotions**
- **Bullying**

9.2 Preventing AI-Generated Harm

AI-generated content, including deepfakes and misinformation, presents new safeguarding challenges. Staff and students must be aware of these risks and trained to respond appropriately (annually at a minimum).

Key requirements:

- AI tools must not be used to create harmful, misleading, or inappropriate content
- Students and staff must be trained to recognise AI-generated deepfakes, misinformation, and impersonation risks
- The school's filtering and monitoring systems must detect and prevent AI-generated threats in accordance with the Government's Filtering and Monitoring Standards

9.3 Reporting Safeguarding Concerns

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately.

Any such incident will be dealt with according to the procedures set out in the school's child protection and safeguarding policy and child protection referral process.

10. Cybersecurity

As AI systems become more integrated into school operations, cybersecurity risks must be managed to prevent unauthorised access, phishing attempts and data breaches.

10.1 AI and Cybersecurity Risks

The school recognises that AI introduces new cybersecurity risks, including:

- **AI-related phishing scams** -- increasingly sophisticated phishing emails generated by AI
- **Fraud** -- AI-generated voice or video used for fraudulent purposes
- **Security vulnerabilities** -- AI tools that may introduce weaknesses in our systems
- **Unauthorised access** -- AI tools that may allow external parties to access school data

10.2 Cybersecurity Measures

The Director of Information & Systems and IT team must:

- Monitor AI-related phishing scams, fraud, and cybersecurity risks
- Ensure AI tools do not introduce security vulnerabilities
- Conduct regular cybersecurity audits to monitor AI-related risks
- Implement security measures to ensure AI tools comply with data protection laws
- Ensure that the school's filtering and monitoring systems detect and prevent AI-generated threats

All staff must:

- Be vigilant for AI-related phishing attempts
- Report any suspected cybersecurity incidents to the IT team immediately
- Follow the school's cybersecurity and online safety policies

11. Staff Training

All staff, governors and relevant stakeholders must engage in annual update training to ensure compliance and risk mitigation for emerging AI risks.

Training will cover:

- Good understanding of AI and its capabilities and limitations
- AI use in staff training on safe internet use and online safeguarding
- Recognising AI bias and hallucinations
- Identifying AI-generated content (including deepfakes, misinformation, and impersonation)
- Data protection and privacy requirements when using AI
- Cybersecurity risks associated with AI
- Safeguarding risks and how to respond
- Ethical and responsible use of AI
- Monitoring student work for signs of AI misuse

Responsibility for training:

- The **AI Lead** will be responsible for ensuring staff have access to continuing professional development (CPD) opportunities on AI.
- The school will stay abreast of good practice through the Key, DfE updates and professional networks and share it with staff through briefings, email updates and INSET training.

12. Breach of This Policy

12.1 By Staff

Breach of this policy by staff will be dealt with in line with our staff code of conduct.

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the Co-Headteachers immediately.

12.2 By Governors

Governors found in breach of this policy will be dealt with by the usual code of conduct procedures.

12.3 By Pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour policy and, if required, our child protection and safeguarding policy.

12.4 Data Breaches

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Droitwich Spa High School and Sixth Form Centre will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

13. Monitoring, Transparency and Review

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the **Director of Information & Systems** and **AI lead** whenever there is a significant change to either AI use by the school or the associated risks of AI usage.

This policy will be:

- Reviewed annually in February, in line with updates to DfE, KCSIE, and JCQ guidance
- Shared with the full governing board at least annually
- Updated to align with emerging best practices, technological advancements and changes in regulations

All teaching staff are expected to read and follow this policy.

The Co-Headteachers and AI lead are responsible for ensuring that the policy is followed.

The Director of Information & Systems will monitor the effectiveness of AI usage across the school.

13.1 Risk Assessments

- Data Protection Impact Assessments (DPIAs) will be conducted before any new AI tools are introduced
- All technologies must undertake a minimum annual DPIA before continued use is permitted

- Annual AI risk assessments will be conducted by the Co-Headteachers and senior leadership team

13.2 Feedback and Evaluation

We will ensure we keep members of the school community up to date on the use of AI technologies for educational purposes.

Feedback will be sought from:

- Pupils
- Parents and carers
- Staff
- Governors

This feedback will be considered in the ongoing evaluation and development of AI use in school through surveys, focus groups and feedback forms.

14. Links with Other Policies

This AI policy is linked to our:

- Data protection policy
- Safeguarding/child protection policy
- Online Safety Policy
- Staff use of ICT Policy
- Assessment policy
- Exams policy
- Homework policy
- Behaviour policy
- Staff code of conduct
- Marking and feedback policy
- ICT acceptable use policy
- Equality policy
- Complaints policy

Droitwich Spa High School and Sixth Form Centre takes its responsibilities as a data controller and data processor seriously and are committed to using any personal data collected and held in accordance with the law. The schools policies, privacy notices and forms in relation to personal data are available for you to view on our web site at www.droitwichspahigh.worcs.sch.uk or by using the <https://website.droitwichspa-high.worcs.sch.uk/index.php/communications/information-management-and-data-protection/> The School's Data Protection Officer is the Head of Governance and Compliance and can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspa-high.worcs.sch.uk