

Policy on

The use of Artificial Intelligence at Lever Edge Primary Academy

This use of AI policy was approved by the Board of Trustees on:	December 2025
The implementation of this AI policy will be monitored by the:	Senior Leadership Team
Monitoring will take place at regular intervals:	As the need arises but at least once a year
The school will monitor the impact of the policy using:	Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity
The Board Trustees will receive a report on the implementation of the AI policy at regular intervals:	At full Board of Trustees Meeting
The AI policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	December 2026 then March 2027 – (when final revised curriculum is due to be released)
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Headteacher/ DSL: Mrs Kelly James LADO: Ms Lisa Kelly Police

Reviewed: January 2026
Next Review: January 2027



Contents

1	Statement of intent	3
2	Related policies	3
3	Policy Statements	3
4	Responsibilities	5
5	Vulnerable groups	6
6	Reporting	6
7	Responding to an incident or disclosure	6
8	Risk assessment	6
9	Education	7
10	Training	8
11	Legislation and guidance	8
A1a	Appendix 1a: AI Tool Evaluation Checklist for School Leaders	10
A1b	Appendix 1b: Risk Assessment Matrix for AI at Lever Edge Primary Academy	13
A2	Appendix 2: Staff Use of AI Acceptable Use Agreement	15
A3	Appendix 3: Staff AI Safety Quick Reference Guide	17



1. Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in, its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations.

We will educate staff and learners about safe, ethical and responsible use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

2. Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Act 2018 / UK GDPR
- Staff Discipline policies and codes of conduct
- Behaviour policy
- Safeguarding / Child protection policy
- SEND policy
- Accessibility Policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements
- Curriculum Policies

3. Policy Statements

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and



sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.

- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school
- AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support learners to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

AI tools will be evaluated for use in school using a checklist which reflects DfE Product Safety Expectations (June 2025) and safeguarding requirements – Appendix 1

Lever Edge primary Academy staff will sign and agree to follow the Staff Use of AI Acceptable Use Agreement – Appendix 2.



4. Responsibilities

4.1 Headteacher and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

4.2 Designated Safeguarding Person (DSP) / Online Safety Lead

Our Designated Safeguarding Person / Online Safety Lead has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

4.3 Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

4.4 Technical Staff

Technical staff (Local Authority technicians) and the school Computing Lead will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

4.5 Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

4.6 Trustees

We ensure that our Trustees have a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

4.7 Parents/carers

We work hard to engage parents and carers by:

- *regular in school sessions*
- *sharing newsletters*
- *sharing information online e.g., website, Class Dojo*
- *providing curriculum information*

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their children's learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.



5. Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be “high risk”. If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

6. Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- nominated member of staff
- established school reporting mechanisms
- online/offline reporting tool
- anonymous/confidential reporting routes
- links to national or local organisations

7. Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school’s normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

8. Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care



9. Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant across the curriculum, predominantly in Computing and PHSE / Jigsaw

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- *Learner assessment*
- *Critical evaluation of emerging trends and research findings*
- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Engaging with learners*
- *Staff training*

The following resources are used:

- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (including updated AI reference)
- ProjectEVOLVE - <https://projectevolve.co.uk>
- UKCIS DSIT "Education for a Connected World"
- Welsh Government - Generative AI – Hwb guidance - Resources, guidance and information for education practitioners, learners, and families on generative AI.

10. Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.



- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Learners Safe."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- We will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age. We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.
- Appendix 3: Staff AI Safety Quick Reference Guide to be shared annually and given to new staff to encourage and refresh good practice.

11. Legislation and guidance

This policy is informed by and compliant with the latest AI, safeguarding and online safety guidance, including:

Statutory Guidance

- DfE Generative artificial intelligence (AI) in education
- Generative artificial intelligence (AI) and data protection in schools
- DfE *Keeping Children Safe in Education (KCSIE) 2025*
- DfE *Teaching Online Safety in Schools*
- *Education for a Connected World (UKCIS Framework)*

Legislation

- *Children Act 1989 & 2004*
- *Computer Misuse Act 1990*
- *Education Act 1996, 2002, 2011*
- *Communications Act 2003*
- *Education and Inspections Act 2006*
- *Equality Act 2010*
- *Data Protection Act 2018 / UK GDPR*

Other Key Guidance

- National Cyber Security Centre (NCSC) guidance for education settings
- Childnet, CEOP, Internet Matters, NSPCC, SWGfL, and other key online safety education partners
- Ofsted's use of AI
- How Ofsted looks at AI during inspection and regulation



AI Tool Evaluation Checklist for School Leaders

This comprehensive checklist has been updated to reflect DfE Product Safety Expectations (June 2025) and safeguarding requirements.

Initial Assessment:

Educational Purpose and Benefits

What educational benefit or improvement does this AI tool provide?

- Describe the specific educational outcome or improvement this tool will deliver
- Identify how it enhances teaching, learning, or administrative processes
- Explain why this particular solution is needed at this time

Target users and context:

- Who will use this tool? (Teachers only / Students only / Both)
- What age groups will it serve?
- Does it generate images or multimodal content?
- Will it be used on personal devices (BYOD) or school-managed devices only?

Section 1: Safety and Security **(Essential Requirements)**

1.1 Content Safety (Essential for child-facing products)

- Tool blocks harmful/inappropriate content generation
- Age-appropriate filtering for your student age groups
- Filtering works across text, images, multiple languages
- Real-time content blocking with user explanations
- Filtering maintained on all devices (including BYOD)

Mark N/A if tool is teacher-only

1.2 Data Protection (Applies to all tools)

- UK GDPR compliant with clear privacy policy

- Explains what data is collected and how it's used
- States where data is processed (UK/EU preferred)
- Confirms data won't be used to train AI without consent
- Provides data deletion on request

1.3 Technical Security (Applies to all tools)

- Meets DfE Cyber Security Standards for Schools
- Strong password/authentication requirements
- Regular security updates and patches
- Administrative controls for user permissions

Section 2: Monitoring and Reporting **(Essential for child-facing products)**

2.1 Activity Monitoring

- Records user activity for safeguarding purposes
- Alerts school staff to harmful content attempts
- Provides real-time notifications when content blocked
- Identifies potential safeguarding disclosures

2.2 Reporting Capabilities

- Provides reports schools can understand and use
- Shows trends in content access attempts
- Has clear incident reporting procedures
- Formal escalation process for safety issues

Mark N/A if tool is teacher-only

Section 3: Educational Suitability **(Applies to all teacher tools)**

3.1 Curriculum Alignment

- Content aligns with UK National Curriculum
- Accurate for intended subjects and age groups
- Age-appropriate content and complexity
- Enhances rather than replaces meaningful learning



- Evidence of positive impact in schools

- Formal complaints and escalation procedures

3.2 Pedagogical Considerations

- Supports rather than replaces teacher expertise
- Encourages critical evaluation of AI outputs
- Supports diverse learning needs and abilities
- Compatible with existing assessment practices
- Provides useful feedback to educators

Mark N/A if tool is leadership-only

Section 4: Intellectual Property Protection

(Applies to all tools)

4.1 Copyright and Creative Work Protection

- Student work protected from unauthorised use
- Teacher work protected from unauthorised use
- Clear consent processes for any data use
- Parental consent for under-18 users where needed
- No commercial use of inputs/outputs without permission
- Clear opt-out from any AI training

4.2 Content Attribution and Copyright

- AI-generated content clearly identified
- Measures to prevent copyright infringement
- Clear content ownership and usage rights
- Respects employer copyright in teacher-created works

Section 5: Transparency and Accountability

(Applies to all tools)

5.1 Explainability and Openness

- Information about training data sources
- Clear explanation of tool limitations
- Acknowledges and addresses potential biases

5.2 Provider Accountability

- Provider demonstrates education sector understanding
- UK regulatory compliance
- Responsive technical and educational support
- Regular updates and improvement processes

Section 6: Design and Testing

(Applies to all tools)

6.1 User-Centred Design

- Child-centred design prioritising safety (*for child-facing tools*)
- Meets accessibility and SEND requirements
- Performs consistently as intended
- Design eliminates discrimination and bias where reasonably possible

6.2 Safety Testing and Validation

- Input from educators and students (child-facing products) in development
- Technical safeguards for identified risks
- Ongoing improvement based on user feedback
- Regular assessment of safety and effectiveness

Section 7: Implementation and Support

(Applies to all tools)

7.1 Technical and Educational Support

- Responsive technical support available
- Guidance on educational implementation
- Comprehensive training programmes

7.2 Change Management and Integration

- Considers staff capacity and skills
- Plans for communicating changes
- Mechanisms to gather user feedback

Section 8: Cost and Sustainability

(Applies to all tools)

8.1 Financial Considerations

- Clear educational benefits justify cost
- All costs transparent (no hidden fees)
- Affordable within school budget
- Good value compared to alternatives
- Potential for measurable return on investment

Scoring and Decision Framework

Scoring Instructions:

✓ Yes - Requirement fully met

✗ No - Requirement not met

- N/A - Not applicable to this tool

Essential Requirements (Must all be "Yes"):

For Child-Facing Tools:

- All Section 1 (Safety and Security) applicable items
- All Section 2 (Monitoring and Reporting) items
- All Section 4 (Intellectual Property) items

For Teacher-Only Tools:

- Section 1.2 and 1.3 (Data Protection and Technical Security)
- All Section 4 (Intellectual Property) items

Recommended Standards:

- Child-facing tools: 90%+ of all applicable items should be "Yes"
- Teacher-only tools: 85%+ of all applicable items should be "Yes"

Total Applicable Items:	_____
Items Scoring "Yes":	_____
Percentage:	_____ %

Evaluator Information:

Name: _____

Role: _____

Review Date: _____

Final Recommendation:

- Approve for implementation - All essential criteria met, benefits clear
- Conditional approval - Approve with specific conditions or limitations
- Further evaluation needed - Requires additional assessment or information
- Reject - Does not meet essential requirements**

Key Conditions/Actions Required:



Risk Assessment Matrix for AI at Lever Edge Primary Academy

Introduction

The following risk assessment matrix is used to help our school identify, evaluate, and mitigate risks associated with implementing Artificial Intelligence (AI) in educational processes.

The matrix considers potential risks across various domains, including data protection, ethical considerations, and operational integrity. There is a particular focus on safeguarding and wellbeing issues, highlighting potential risks to student welfare and offers strategies to mitigate these risks effectively.

Risk Assessment Matrix

Risk Area	Risk Description	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (Low/Med/High)	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.				Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.				Monitor AI communication tools, implement clear reporting mechanisms, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.				Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulation	AI systems unintentionally affecting student mental health through curated content.				Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing learners to harmful or unsuitable materials / behaviour				Conduct rigorous testing of AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.				Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or inclusion. AI models producing discriminatory or biased outcomes.				Regularly audit AI algorithms for bias and provide inclusive media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).				Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or				Educate staff and learners to verify AI outputs



	misleading AI-generated content.				and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among learners from diverse demographic groups.				Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.				Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.				Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and learner data.				Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.				Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Likelihood and Impact Definitions

- **Likelihood:** The likelihood that the identified risk will occur.
 - Low: Unlikely to occur under normal circumstances.
 - Medium: Possible occurrence based on past trends or vulnerabilities.
 - High: Likely to occur without intervention.
- **Impact:** The severity of impact should the risk materialise.
 - Low: Minimal disruption with limited consequences.
 - Medium: Moderate disruption affecting key processes.
 - High: Significant disruption with severe consequences.

Action Plan

Based on the findings of the risk assessment matrix a plan will be agreed; these actions might include

1. Appoint a safeguarding lead to oversee AI implementation and its impact on student welfare.
2. Deliver regular training for staff on online safety, AI ethics, and responsible use.
3. Audit the curriculum to identify where these AI related issues might be incorporated into existing or new curricular programmes.
4. Establish transparent reporting mechanisms for any safeguarding or wellbeing concerns linked to AI.
5. Collaborate with parents and carers to raise awareness about AI risks and best practices.
6. Conduct annual reviews of AI tools and their impact on student wellbeing, updating the risk matrix as needed.

Review and Update

The school will review and update this matrix alongside the Policy on the use of Artificial Intelligence at Lever Edge Primary Academy or whenever new AI technologies or safeguarding challenges arise.



Staff Use of AI Acceptable Use Agreement

Artificial Intelligence (AI) and Emerging Technologies Staff (and Volunteer) Acceptable Use Agreement

Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalised learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of AI.
- Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of AI tools and technologies.
- I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g., UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.
- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using AI systems.
- I will ensure transparency through appropriate attribution where AI has been used.



When engaging with learners:

- I will support learners on the safe, ethical, appropriate and effective use of AI.
- I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use AI systems in compliance with established security measures and access protocols.
- I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.
- I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.
- I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

- I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

I have read and understand the above and agree to apply it when using AI technology in school, as well as out of school when undertaking work related activities and using work devices.

Name:

Signed:

Date:



Appendix 3

Staff AI Safety Quick Reference Guide

This quick reference guide provides essential safety information for all staff using AI tools in educational settings.

Recognising AI Limitations

Remember: AI is a tool to enhance human expertise, not replace it. When in doubt, ask for help!

Essential Safety Rules

NEVER Do These Things:

- Input personal data into **unapproved** AI tools or free personal AI accounts
- Use free, consumer AI tools (ChatGPT, Gemini, etc.) for school work involving personal data
- Upload student work to unapproved tools without proper permissions and safeguards
- Share AI-generated content without checking for accuracy and appropriateness
- Allow unsupervised pupil access to AI tools without proper safeguards
- Rely solely on AI outputs without human verification
- Use AI for final decisions about students without human review

ALWAYS Do These Things:

- Use only approved AI tools provided by the school
- Verify that approved tools have appropriate data protection measures (e.g., no model training on user data)
- Check all AI outputs for accuracy, bias, and appropriateness
- Maintain human oversight of all AI-assisted work
- Report concerns immediately to DSL or senior leadership
- Follow data protection guidelines when using any AI tool
- Be transparent about AI use with students and colleagues
- Keep learning about AI developments and best practices

Watch Out For:

- **Hallucinations:** AI making up convincing but false information
- **Bias:** Unfair representation of groups or individuals
- **Outdated information:** AI training data may be months or years old
- **Context misunderstanding:** AI may not grasp local or specific situations
- **Inappropriate content:** Despite filters, concerning content may occasionally appear

Red Flags in AI Outputs:


- Unusual facts without sources
- Content that seems "too good to be true"
- Stereotypical representations
- Inconsistent information
- Overly complex or simple language for the context

Data Protection Quick Check

Before Using Any AI Tool, Ask:


- Is this tool approved by our school?
- Does this tool have appropriate data protection measures in place?
- If using personal data, is this tool specifically approved for such use?
- Could this data be used to train the AI model inappropriately?
- Do I have permission to use any copyrighted content?
- Is there a non-AI way to accomplish this task?

Understanding Tool Categories:

 **Approved tools with data protection** (e.g., school MIS system with AI features, enterprise AI tools with no-training policies etc):

- May be used with personal data as per school policy
- Still require appropriate professional judgement
- Must follow any specific usage guidelines



 **Approved tools without data protection** (general AI tools):

- Use placeholder names (e.g., "Student A," "The teacher")
- Remove identifying details from any text
- Anonymise data before inputting

 **Unapproved tools:**

- Never use for school work
- Never input any school-related data

Safeguarding Checklist

If You Encounter Concerning Content:

- Don't panic - take a screenshot if safe to do so
- Stop using the tool immediately
- Report to DSL or senior leadership
- Document what happened and what you were trying to do
- Follow normal safeguarding procedures

Warning Signs to Report:

- Generation of inappropriate images or text
- Content that could be used for grooming or exploitation
- Discriminatory or hateful outputs
- Content promoting harmful activities
- Any output that raises safeguarding concerns

Academic Integrity Guidelines

When Working with Students:

- Be clear about when AI use is/isn't appropriate
- Teach students to identify AI-generated content
- Model critical evaluation of AI outputs
- Emphasise the importance of human thinking and creativity
- Check work for signs of AI assistance when inappropriate

Signs of Potential AI Misuse in Student Work:

- Sudden improvement in writing quality
- Unusual vocabulary or writing style
- Lack of personal voice or perspective
- Perfect grammar in otherwise inconsistent work
- References or information that seem out of place

Who to Contact:

Issue Type	Contact	When
Technical problems	IT Support	During work hours
Safeguarding concerns	DSL	Immediately
Data protection questions	DPO	Before using new tools
Training needs	Line Manager	Ongoing
General AI questions	AI Lead/Senior Leader	Any time

Resources Available:

- DfE AI Toolkit Modules (mandatory for all staff)
- School AI Policy (available on staff intranet)
- Regular CPD sessions on AI use
- Peer support networks within school
- External training opportunities as available

Quick Decision Tree

Thinking of using AI? Follow this process:

1. **Is this an approved tool?** → If NO, stop here
2. **Do I need to input personal data?** → If YES, check it's approved for personal data use
3. **Will this enhance rather than replace my professional judgement?** → If NO, reconsider
4. **Can I check and verify the output?** → If NO, don't use
5. **Is this transparent and ethical?** → If NO, find another approach
6. **Will this genuinely save time or improve outcomes?** → If YES, proceed with caution

Regular Review Questions

Ask yourself monthly:

- Am I using AI tools safely and effectively?
- Have I kept up with training and policy updates?
- Am I modelling good AI practices for students?
- Are there new AI-related risks I should be aware of?
- Do I need additional support or training?