



EDUCATION
EAST SUSSEX
TOGETHER FOR EXCELLENCE
AND INCLUSION



AI and Emerging Technology Procedure

Alfriston Primary School

This policy was adopted on 30th September 2026

This policy is due for review on 1st September 2027



Contents

1. Purpose and scope.....	4
2. Definitions	5
3. Legal and guidance framework	5
4. Principles for safe and responsible use.....	6
5. Approval categories: permitted, approval required and prohibited use	7
6. Staff use of AI	8
7. Pupil and learner use	9
8. Safeguarding and online safety risks.....	10
9. AI-generated sexual imagery, deepfakes and impersonation	11
10. AI-enabled smart devices, smart wearables and connected technology	12
11. Data protection, confidentiality and privacy	13
12. Accuracy, bias, transparency and human oversight.....	14
13. Intellectual property, copyright and ownership	14
14. Assessment and academic integrity	15
15. Procurement and approval of AI-enabled technology	15
16. Filtering, monitoring and cyber security	16
17. Reporting concerns and incidents	16
18. Training and awareness	18
19. Monitoring, review and emerging technology.....	18
Appendix A. AI and emerging technology approval checklist.....	20
Appendix B. Staff decision guide: Can I use AI for this?.....	22

AI and Emerging Technology Procedure

Appendix C. Example red / amber / green uses	23
Appendix D. Guidance and statutory reference framework	25

1. Purpose and scope

This procedure explains how the setting will use artificial intelligence (AI) and emerging technologies safely, lawfully and appropriately. It supports the Core Online Safety Policy by translating high-level principles into practical expectations for staff, children and learners, leaders, technical teams and third-party providers.

The procedure applies whether AI is used as a standalone service or is embedded within a wider product, platform or device. It covers, where relevant:

- generative AI tools that create or transform text, images, audio, video, code or other content;
- AI chatbots, digital assistants and AI companions;
- AI features embedded in learning platforms, search engines, productivity software, communications systems and management tools;
- automated decision-support, personalisation, profiling, recommendation or analytics tools;
- AI-enabled smart devices and connected technology, including smart watches, smart glasses, wearable cameras, voice assistants, connected toys, health or fitness wearables and similar devices;
- augmented reality (AR), virtual reality (VR) and mixed-reality systems where they use AI-enabled features;
- AI-enabled assistive technology and accessibility tools; and
- new or emerging technologies that create comparable safeguarding, privacy, security, educational or ethical risks.

This procedure does not assume that all AI use is either safe or unsafe. Controls should reflect the purpose, users, age, vulnerability, data involved, technical capability and likely impact.

2. Definitions

Term	Meaning
Artificial intelligence (AI)	Digital systems that perform tasks involving pattern recognition, prediction, recommendation, content generation or conversational response.
Generative AI	AI that creates new content such as text, images, audio, video, code or synthetic data in response to prompts or other inputs.
AI-enabled smart device	A physical device with embedded or connected AI capability, such as a voice assistant, smart camera, connected toy, sensor or other device that can collect, interpret, generate or respond to data.
Smart wearable	Technology worn on the body that may communicate, record, sense, track or process information, including smart watches, smart glasses, wearable cameras, health or fitness wearables and AI-enabled assistive devices.
Deepfake	Synthetic or manipulated audio, image or video designed to make a person appear to say or do something they did not say or do.
Nudification / synthetic sexual imagery	Use of AI or image manipulation to create or alter an image so that a person appears nude, semi-nude or sexualised.
Automated decision-making	A decision made solely by automated means without meaningful human involvement. Data protection law places specific requirements on certain forms of solely automated decision-making.
Profiling	Automated processing of personal data to evaluate or predict aspects of a person's behaviour, performance, interests, health, preferences or other characteristics.
Approved tool	A tool, service or device that has passed the setting's relevant safeguarding, data protection, security, accessibility and procurement checks for the proposed use.

3. Legal and guidance framework

There is no single statutory requirement for every education setting to adopt a standalone AI policy. The requirements relevant to AI arise from the wider legal and statutory

framework that applies to safeguarding, data protection, behaviour, equality, procurement and the setting's use of technology.

The procedure should be read in the context of:

- Keeping Children Safe in Education (KCSIE), including its expectations for online safety, filtering and monitoring, staff training and safeguarding response;
- UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025;
- DfE guidance on Generative artificial intelligence in education and the Safe use of generative AI in education support materials;
- DfE Data protection in schools guidance, including Generative AI and data protection in schools and (EdTech);
- DfE Filtering and monitoring: core standard and Cyber security: core standard;
- DfE Generative AI: product safety standards, which are primarily written for developers and suppliers but may support settings when assessing products;
- statutory Mobile phones in schools guidance where it applies; and
- other applicable safeguarding, equality, intellectual property, assessment and local requirements. Procuring educational technology

Please Note - In this procedure, 'must' is used for a legal or statutory requirement, or for a mandatory local control established by this procedure. 'Should' reflects DfE guidance or recommended practice. 'May' indicates local discretion.

4. Principles for safe and responsible use

- Human accountability: people remain responsible for decisions, professional judgement and safeguarding action. AI does not replace professional expertise.
- Safeguarding first: the welfare of children and learners takes priority over convenience, innovation or efficiency.
- Purpose before tool: users should identify the educational or organisational need before deciding whether AI is appropriate.
- Minimum necessary data: personal data should not be entered into generative AI tools unless there is an approved, lawful and necessary reason.
- Age and vulnerability: access, supervision and teaching must reflect age, maturity, SEND, communication needs and individual vulnerability.
- Transparency: users should understand when AI is being used and, where personal data is processed, the setting must meet applicable transparency requirements.
- Critical review: AI output must be checked for accuracy, bias, appropriateness, fabricated information and unsafe content before use.

- Security and privacy by design: tools and devices should be approved and configured so that unnecessary data collection, retention, sharing or exposure is minimised.
- Accessibility and inclusion: controls must not unnecessarily restrict legitimate assistive technology or reasonable adjustments.
- Continuous review: AI capability changes quickly; approvals must be revisited when suppliers add new features or alter data processing.

5. Approval categories: permitted, approval required and prohibited use

The setting should maintain a simple local approval model so staff can tell whether a proposed use is routine, needs additional review, or is not allowed.

Category	Meaning	Examples	Action
GREEN - generally permitted	Low-risk use of an approved tool with no personal, confidential or safeguarding data and no high-stakes decision-making.	Generating generic lesson ideas; simplifying non-personal text; drafting generic quiz questions; brainstorming; producing a first draft of non-confidential administrative text.	Use professional judgement, check output and follow normal acceptable-use requirements.
AMBER - approval required	Use creates additional safeguarding, privacy, assessment, security, accessibility or reputational risk.	Pupil-facing AI; tools processing pupil information; AI-enabled smart devices or wearables; personalised learning; automated analytics; image or voice generation involving identifiable people; assessment or feedback uses; new AI features in existing systems.	Seek approval through the local process before use. Involve the DSL/DDSL, DPO, IT/digital lead and curriculum lead as appropriate.
RED - prohibited	Use conflicts with law, safeguarding duties, professional standards	Entering safeguarding records into an unapproved public AI	Do not proceed. Report concerns or incidents where

Category	Meaning	Examples	Action
	or setting rules.	tool; creating sexualised images; covertly recording people with AI-enabled wearables; impersonating a person; bypassing filtering or security; using AI for a solely automated high-stakes decision where this is not lawful or approved.	relevant.

6. Staff use of AI

Staff may use approved AI tools where the use supports a legitimate educational or organisational purpose and complies with this procedure, data protection requirements and professional standards.

Staff must

- use approved organisational accounts, tools and devices where these are required;
- check the age, intended use and terms of the product before directing pupils to use it;
- critically review output before it is used, shared or relied upon;
- check factual claims, references and citations rather than assuming AI-generated material is correct;
- ensure AI-generated learning material is suitable for the age, needs and curriculum context of the intended learners;
- remain responsible for feedback, assessment judgements, safeguarding decisions, disciplinary decisions and other professional conclusions;
- comply with copyright, licensing and intellectual property requirements;
- be transparent about significant AI use where this is necessary for accountability, assessment, data protection or professional integrity; and
- report harmful output, privacy incidents, account compromise or safeguarding concerns through the relevant route.

Staff must not

- use AI to replace professional safeguarding judgement or to decide whether a safeguarding concern should be reported;
- upload child protection records, medical details, special category data, confidential HR material, unpublished assessment material or other sensitive information into an unapproved AI service;
- enter personal, confidential, special category or safeguarding information unless the use has been explicitly approved and the required data protection controls are in place;
- create deceptive, sexualised, humiliating, discriminatory or harmful content involving pupils, colleagues or members of the community;
- use AI to impersonate another person or to create synthetic communications that could reasonably mislead recipients about authorship;
- use personal accounts, smart devices or wearables to circumvent setting controls; or
- allow convenience to override approved procurement, privacy, security or safeguarding processes.

7. Pupil use

Pupil use of AI should be age-appropriate, purposeful, supervised where required and consistent with the terms and age restrictions of the product. DfE guidance states that pupils should use generative AI only with appropriate safeguards in place, such as suitable supervision and tools with safety, filtering and monitoring features.

- Pupils should use only the AI tools, accounts and features authorised for their age and educational activity.
- Younger pupils and pupils who require additional support should receive a level of supervision proportionate to risk and need.
- Pupils should be taught that AI can be inaccurate, biased, persuasive or manipulative and that generated content may appear convincing even when false.
- Pupils must not enter another person's personal or confidential information into AI tools without permission and an approved educational reason.
- Pupils must not use AI to create, request, alter or share sexualised images, deepfakes, abusive content, impersonations or material intended to humiliate, harass, deceive or exploit.
- Pupils should understand when AI use is permitted in assessed work and when acknowledgement or declaration is required.

AI and Emerging Technology Procedure

- Pupils should know how to report harmful outputs, unsafe interactions, requests for personal information, sexual content, coercive behaviour, distressing AI companion interactions or other concerns.
- Pupils using AI-enabled assistive technology should be supported through reasonable adjustments and individual risk assessment where necessary.

EYFS and KS1

- No direct pupil use of generative AI.
- Teachers may demonstrate age-appropriate examples.
- AI may be used by staff to generate resources.

KS2

- Teacher-led demonstrations only.
- Whole-class activities using a shared screen.
- Focus on understanding:
 - what AI is
 - that AI makes mistakes
 - why we check information

8. Safeguarding and online safety risks

AI can create new forms of harm or intensify existing online safety risks. Concerns should be understood through the same safeguarding framework used for other online and offline harm.

Risk area	Examples
Content	Harmful, illegal, sexual, violent, extremist, hateful, self-harm or suicide content; inaccurate or fabricated information; age-inappropriate output; synthetic media.
Contact	Unsafe chatbots or AI companions; systems that facilitate contact with unknown users; grooming, coercion or exploitation enabled by AI; persuasive or emotionally manipulative interactions.
Conduct	Deepfakes, nudification, sexualised image manipulation, impersonation, cyberbullying, harassment, doxxing, fraud, cheating, abusive prompts or use of AI to scale harmful behaviour.
Commerce	AI-enabled scams, phishing, fraud, impersonation,

Risk area	Examples
	financial manipulation, deceptive marketing or subscription practices.
Privacy and surveillance	Excessive collection of voice, image, location, biometric, health or behavioural data; hidden recording or tracking; profiling or inappropriate automated analysis.
Development and wellbeing	Over-reliance, emotional dependency, reduced critical thinking, harmful reinforcement, manipulative design, social displacement or adverse mental-health effects.

Where AI use raises a safeguarding concern, staff should respond to the underlying harm rather than treating the incident as merely a technology issue.

9. AI-generated sexual imagery, deepfakes and impersonation

AI-generated or manipulated sexual imagery involving a child, including nudification or deepfake sexual imagery, is a safeguarding concern and may also involve criminal or other legal issues. The response must follow the setting's Incident Response Procedure and relevant safeguarding guidance.

Staff must not create, request, share, copy, print, save or unnecessarily view sexualised or nude/semi-nude imagery of children.

A child should not be asked to send or forward an image to a member of staff in order to prove what has happened.

Staff should protect the child, avoid unnecessary exposure, preserve relevant information where safe and lawful, and report promptly to the DSL.

The DSL should consider coercion, exploitation, sexual extortion, peer abuse, adult involvement, distribution, threats, vulnerability and whether statutory agencies need to be involved.

Impersonation, cloned voices, fake accounts and deepfake video or audio should be treated according to the harm caused or intended, including safeguarding, fraud, harassment, staff conduct or cyber-security routes as appropriate.

10. AI-enabled smart devices, smart wearables and connected technology

AI capability is increasingly embedded in physical devices. Smart watches, smart glasses, wearable cameras, voice assistants, connected toys, health or fitness wearables, AR/VR headsets and AI-enabled assistive technology may collect, infer, record or transmit information even when they are not being used in the same way as a conventional computer.

Before such technology is introduced or permitted for organisational use, the setting should consider:

- whether the device can record audio, video or images, and whether recording is obvious to people nearby;
- whether it processes location, biometric, health, behavioural, facial, voice or other personal data;
- whether information is stored or processed locally, in the cloud, or transferred internationally;
- whether the device can respond to voice, generate content, identify people or objects, summarise conversations or make recommendations;
- whether it can communicate, message, connect independently to mobile networks or bypass setting filtering, monitoring or network controls;
- whether the device has an appropriate educational, accessibility or operational purpose;
- whether the use is consistent with the setting's Mobile Phone and Personal Device Policy, image-use rules, assessment rules and cyber-security requirements; and
- whether reasonable adjustments are required for disabled pupils or staff.

Where the statutory Mobile Phones in Schools guidance applies, references to mobile phones can also apply to other communications and smart technology that the school has decided to include in its policy. Schools should therefore decide explicitly which smart watches, smart glasses and other devices with similar communications or recording functionality are within scope.

AI-enabled assistive technology must not be restricted simply because it contains AI. The setting should assess the actual safeguarding, privacy and security risks and consider its equality and reasonable-adjustment duties.

11. Data protection, confidentiality and privacy

AI tools and AI-enabled devices may process personal data in the information entered by a user and may also collect additional information such as IP address, location, device, browser, voice, image or system information. Use must comply with data protection law and the setting's privacy framework.

Personal data

- The setting must identify the lawful basis for processing personal data and meet transparency requirements.
- Staff should avoid using personal data in generative AI tools unless it is strictly necessary and the use has been approved.
- Where personal data is used, the setting must understand how the supplier processes, stores, shares, retains and uses the data, including whether data may be used to train a model.
- Privacy notices and records of processing should be updated where necessary.
- A DPIA must be completed where processing is likely to result in a high risk to individuals' rights and freedoms. This is particularly relevant to high-risk profiling, large-scale biometric processing or other intrusive uses.
- The DPO must be involved at an early stage in relevant procurement and implementation decisions.

Biometric, health and location data

AI-enabled smart devices and wearables may process biometric, health, location or behavioural data. Some of this may be special category data. The setting must therefore understand exactly what the device collects and why before approving organisational use.

Automated decision-making and profiling

Where AI is used to profile pupils or support automated decisions, the setting must assess the applicable data protection requirements and ensure meaningful human oversight where required. High-stakes decisions about safeguarding, discipline, admissions, educational support or similar matters must not be delegated to an AI tool merely because it can generate a recommendation.

12. Accuracy, bias, transparency and human oversight

AI outputs may be inaccurate, incomplete, biased or fabricated. Users must therefore apply professional and critical judgement.

- Check factual claims, calculations, citations and references against reliable sources where accuracy matters.
- Do not assume a confident or fluent response is correct.
- Consider whether outputs reproduce stereotypes, discrimination or bias, particularly where children with protected characteristics or additional needs may be affected.
- Do not use AI output as the sole basis for a safeguarding, disciplinary, employment, assessment or other high-impact decision.
- Where an AI system influences a decision about a person, the setting should be able to explain the role the system played and the human judgement applied.
- Users should be open about material AI assistance where required by assessment rules, organisational policy, professional integrity or data protection transparency obligations.

13. Intellectual property, copyright and ownership

The fact that content has been generated by AI does not remove intellectual-property considerations. Staff and learners must follow applicable copyright, licensing and attribution requirements.

- Do not upload copyrighted, licensed or confidential material (including pupil work) to an AI service unless the proposed use is authorised.
- Check supplier terms for rights over prompts, uploaded material and generated output.
- Do not assume AI-generated images, text, audio, video or code are free from third-party rights.
- Where AI is used to adapt or create teaching material, staff remain responsible for checking whether the output is appropriate to use and share.
- Pupils should be taught to acknowledge AI use where required and to distinguish their own work from machine-generated material.

14. Assessment and academic integrity

AI may support learning, but its use in assessed work must comply with the rules of the relevant awarding organisation and the setting's assessment or malpractice procedures.

- Staff should explain clearly when AI use is permitted, restricted or prohibited in an assessment.
- Where disclosure or acknowledgement is required, learners must identify the AI assistance used.
- Submitting AI-generated work as a learner's own where this is not permitted may constitute malpractice.
- Staff should not rely solely on AI-detection tools to determine whether malpractice has occurred; concerns should be considered using the evidence and procedures required by the relevant qualification framework.
- Settings delivering regulated qualifications should maintain a consistent whole-setting approach to AI and coursework integrity, informed by current Ofqual and awarding-body guidance.

15. Procurement and approval of AI-enabled technology

AI should be identified during procurement even when it is only one feature within a wider EdTech product, smart device or wearable. DfE data protection guidance requires schools to assess how AI is used in EdTech and to consult the DPO and DSL before deciding whether to procure an AI-enabled tool.

Before approval, the setting should establish:

- the intended educational or organisational purpose and the users who will access the product;
- the age restrictions and whether the product is suitable for the intended learner group;
- whether the product generates content, responds to pupil information, personalises learning, profiles users or uses automated decision-making;
- what personal data is collected, where it is stored, how long it is retained and whether it is used to train the model;
- how harmful, inappropriate, inaccurate or biased output is moderated and what controls the setting can configure;

- whether authorised staff can provide appropriate monitoring and supervision;
- the product's filtering, reporting, security, account and access-control capabilities;
- whether the product creates risks to cognitive development, emotional and social development, mental health or manipulation;
- the implications for copyright, intellectual property and licensing;
- accessibility, SEND and reasonable-adjustment implications;
- supplier responsibilities, contractual controls and incident-reporting arrangements; and
- whether a DPIA, risk assessment or other formal approval is required before implementation.

Approval must be reviewed when the supplier materially changes AI functionality, data processing, age restrictions, integrations or safety controls.

16. Filtering, monitoring and cyber security

AI use must be considered within the setting's filtering, monitoring and cyber-security arrangements. DfE's filtering and monitoring core standard requires schools and colleges to consider whether solutions capable of handling real-time, dynamic, personalised and AI-generated content are required and to assess the risks of generative-AI tools.

- The annual filtering and monitoring review should consider how AI tools are used and any technical limitations affecting AI-generated or in-app content.
- AI-enabled devices and wearables that connect to organisational networks should be subject to appropriate network, account and device controls.
- Personal mobile data, unmanaged connections or smart-device features must not be used to circumvent the setting's filtering, monitoring or security arrangements.
- AI-enabled services should use approved accounts and authentication arrangements where required.
- Cyber incidents involving AI, including phishing, impersonation, account compromise or malicious generated content, should be managed under the Cyber Security and Account Management Standard.

Detailed technical requirements belong in the Filtering and Monitoring Standard and Cyber Security and Account Management Standard and are not repeated here.

17. Reporting concerns and incidents

Staff and learners should report concerns promptly. The response route depends on the

nature of the issue.

Concern	Primary route	Immediate principle
Harmful or sexual AI-generated content involving a child	DSL / safeguarding team	Follow the Incident Response Procedure. Do not investigate unnecessarily or ask the child to forward sexual imagery.
Deepfake, nudification, impersonation, sexual extortion or coercion	DSL / safeguarding team	Assess underlying safeguarding harm, peer/adult involvement and whether police or other statutory agencies are required.
Personal data entered into an AI service unexpectedly or without approval	DPO / Data Protection Lead and relevant senior lead	Treat as a potential data-protection incident and assess containment, deletion, supplier contact and breach obligations.
Suspicious AI-generated email, message, voice clone or payment request	IT / cyber incident route	Treat as a possible phishing, fraud or account-compromise incident; involve safeguarding where a child is affected.
Unsafe chatbot or AI companion interaction	DSL / safeguarding team	Consider emotional harm, coercion, sexual content, self-harm, grooming and the child's vulnerability.
Unapproved AI tool or smart device used in setting activity	Relevant senior / digital lead	Stop or contain the use where necessary and assess safeguarding, privacy, security and educational risk before any future approval.
Lost or compromised AI-enabled smart device / wearable	IT / DPO / DSL as relevant	Consider data exposure, remote access, recording, location and safeguarding implications.
AI output used in assessed work contrary to rules	Assessment / examinations lead	Follow the relevant awarding-body and

Concern	Primary route	Immediate principle
		malpractice procedures.

18. Training and awareness

Staff training should be proportionate to role and use. DfE's Safe use of generative AI in education materials cover safeguarding, ethics, data and intellectual property and are suitable for staff awareness.

- All staff should understand the setting's basic AI rules, approved-use route, privacy expectations and safeguarding-reporting route.
- Staff who use AI should understand limitations including hallucination, bias, persuasive output and confidentiality risks.
- DSLs and safeguarding staff should understand AI-enabled harms including deepfakes, nudification, AI companions, manipulation and synthetic impersonation.
- Digital/IT and DPO roles should receive sufficient information to assess AI-enabled products, integrations, smart devices and wearables.
- Staff involved in assessment should understand current qualification and malpractice rules relating to AI.
- Children and learners should receive age-appropriate teaching about critical use, privacy, harmful content, academic integrity and reporting concerns.

19. Monitoring, review and emerging technology

AI functionality can change rapidly, including through updates to products already in use. The setting will therefore review this procedure at least annually and sooner where significant changes occur.

Review should consider:

- new statutory or DfE guidance;
- changes in supplier terms, data processing, age restrictions, model behaviour or safety features;
- new AI functions embedded in existing platforms, apps or devices;
- new smart glasses, smart watches, wearable cameras, voice assistants, connected

- toys, health/fitness devices, AR/VR tools and AI-enabled assistive technology;
- patterns identified through safeguarding incidents, filtering and monitoring reports, cyber incidents, complaints or pupil voice;
- new forms of synthetic sexual imagery, impersonation, fraud, manipulation or harmful AI companion behaviour;
- accessibility and equality implications; and
- whether approved tools remain necessary, proportionate and fit for purpose.

Appendix A. AI and emerging technology approval checklist

Check	Questions	Decision / evidence
Purpose	What problem or educational need does the product solve? Is AI necessary for that purpose?	[Insert]
Users	Who will use it: staff, pupils, parents or external users? What age groups and vulnerabilities are relevant?	[Insert]
Age restrictions	Do the supplier's age requirements permit the proposed use?	[Insert]
Safeguarding	Could users encounter harmful content, unsafe chatbots, strangers, sexual material, deepfakes, manipulation or other online-safety risks? What safeguards are in place to ensure inappropriate content is not shown to users?	[Insert]
Smart device / wearable functions	Can it record, photograph, locate, identify, track, transcribe, summarise, message or communicate independently?	[Insert]
Personal data	What pupil, staff or parent data is processed? Does it include special category, biometric, health, location, voice or image data?	[Insert]
Training data	Are prompts, uploads or user data used to train or improve the model? Can this be disabled contractually or technically?	[Insert]
DPIA	Is processing likely to result in high risk to individuals' rights and freedoms?	[Insert]
Human oversight	Can staff supervise and intervene? Are any decisions automated or based on profiling?	[Insert]
Filtering and monitoring	Can the tool or device be appropriately filtered, monitored or supervised? What are the technical limitations?	[Insert]

Check	Questions	Decision / evidence
Security	How are accounts, authentication, access, updates, integrations and incident notifications managed?	[Insert]
Accuracy and bias	What does the supplier do to mitigate inaccurate or biased output? What checks will staff apply?	[Insert]
IP and copyright	Who owns inputs and outputs? What licences or restrictions apply?	[Insert]
Accessibility	Is it accessible? Could controls disadvantage disabled users or interfere with assistive technology?	[Insert]
Supplier assurance	Are responsibilities clear in contracts and privacy documentation?	[Insert]
Approval and review	Who approves the use, what conditions apply and when will it be reviewed?	[Insert]

Appendix B. Staff decision guide: Can I use AI for this?

1. Is the tool or device approved for this purpose and user group? If no, stop and seek approval.
2. Will you enter, upload, capture or expose personal, confidential, safeguarding, health, biometric, location or other sensitive information? If yes, consult the DPO / relevant lead before proceeding unless the use is already formally approved.
3. Will a child use or interact with the tool? Check age restrictions, supervision, safety features and filtering/monitoring arrangements.
4. Is this a smart device or wearable? Check recording, messaging, location, biometric, health and mobile-data functions and the Mobile Phone and Personal Device Policy.
5. Will the AI influence a safeguarding, disciplinary, assessment or other high-impact decision? Ensure meaningful human judgement and follow the relevant procedure.
6. Could the use create deepfakes, impersonation, harmful content or manipulation? If yes, do not proceed unless the use is specifically authorised and safeguarded; report any concern.
7. Can you check the output for accuracy, bias, copyright and appropriateness before using it? If no, do not rely on it.
8. Do you need to acknowledge or record AI use for assessment, professional integrity, procurement or transparency? If yes, do so.
9. If the purpose, risks or controls are unclear, ask the setting's named AI/digital lead, DSL, DPO or IT lead before use.

Appendix C. Example red / amber / green uses

Category	Example	Position
GREEN	Teacher uses an approved AI tool to generate generic starter questions using no personal data.	Permitted subject to checking accuracy and suitability.
GREEN	Administrator uses an approved tool to improve the wording of a generic letter, adding names only after the AI output is complete.	Permitted if no personal data is entered into the AI tool.
AMBER	Teacher wants pupils to use a chatbot during a lesson.	Check age restrictions, educational purpose, supervision, safety features, privacy and filtering/monitoring before approval.
AMBER	Setting wants to use smart glasses or an AI wearable for an accessibility need.	Assess recording, privacy, network and safeguarding risks and consider reasonable-adjustment duties; do not impose a blanket ban.
AMBER	School considers an AI-enabled learning platform that profiles pupils and personalises tasks.	DPO and DSL involvement required; assess data protection, safeguarding, profiling, bias, human oversight and supplier controls.
AMBER	Staff want AI to draft individual pupil feedback using identifiable pupil work.	Requires an approved workflow and data-protection assessment; the teacher remains responsible for the feedback.
RED	Member of staff uploads a safeguarding chronology to a public AI chatbot to summarise it.	Prohibited unless an explicitly approved secure system and lawful workflow exists.
RED	Pupil uses AI to create a sexualised image of another pupil.	Safeguarding concern; follow the Incident Response Procedure.

AI and Emerging Technology Procedure

Category	Example	Position
RED	User wears an AI-enabled camera or smart glasses to covertly record pupils or staff contrary to setting rules.	Prohibited local use and potentially a safeguarding / privacy concern.
RED	AI is used as the sole basis for deciding whether a safeguarding disclosure is credible.	Prohibited: safeguarding decisions require human professional judgement.

Appendix D. Guidance and statutory reference framework

Source	Status	Relevance
Keeping Children Safe in Education 2026	Statutory guidance	Published 7 July 2026; comes into force 1 September 2026.
UK GDPR and Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025	Law	Applies to processing of personal data; DUAA changes came into force in July 2026.
Generative artificial intelligence (AI) in education	DfE guidance	Schools and colleges choose suitable AI uses subject to wider statutory duties; pupils should use AI with appropriate safeguards and age restrictions must be observed.
Data protection in schools: Generative AI and data protection in schools	DfE guidance	Covers personal data, transparency, tool approval, age restrictions, AI data collection, profiling and automated decisions.
Data protection in schools: Procuring educational technology (EdTech)	DfE guidance	Requires data protection compliance in procurement and says DPO and DSL should be consulted before deciding to procure AI-enabled EdTech.
Generative AI: product safety standards	DfE guidance / supplier standards	Primarily for developers and suppliers; settings may use them to assess products. Includes filtering, monitoring, security, privacy, IP, governance, cognitive development, emotional/social development, mental health and manipulation.
Filtering and monitoring: core standard	DfE digital and technology standard	Updated in June 2026 to clarify assessment of generative-AI risks and limitations.
Cyber security: core standard	DfE digital and technology standard	Sets expectations for cyber-security controls and governance.
Mobile phones in schools	Statutory guidance	Became statutory 29 June 2026; schools should begin following from

AI and Emerging Technology Procedure

Source	Status	Relevance
		1 September 2026. References can include other communications and smart technology chosen by the school.
Safe use of generative AI in education: module 3	DfE training/support material	Covers safeguarding, ethics, data and intellectual-property risks.
AI in coursework: resources for schools	Ofqual guidance/resources	Supports a whole-setting approach to AI and coursework integrity; regulated qualification rules and awarding-body requirements also apply.