AI & EMERGING TECHNOLOGIES POLICY

Policy Owner:	Chief Operating Officer (COO)
ISSR Reference:	Part 2 – Spiritual, Moral, Social and Cultural Development of Pupils Part 3 – Welfare, Health and Safety of Pupils Part 8 – Quality of Leadership in and Management of Schools
Date of review:	Summer 2026
Approved by:	Group Board
Date of next review	Autumn 2026

Version Control Information

Reason for Amendment	Role	Date	Main Changes
New Tier 1 policy formatted into SDEG house style and running order	Chief Operating Officer (COO)	Group Board – Summer 2026	Streamlined format, monitoring wording and policy links aligned to house style Establishes a Group-wide governance framework for AI and emerging technologies, including educational use, safeguarding, data protection, assessment integrity, supplier standards and assurance.

1. Aims

Artificial intelligence is not principally a technology issue. It is an educational, safeguarding, ethical and leadership issue. SDEG will use AI and emerging technologies where they support human flourishing, strengthen education, improve accessibility, enable creativity, reduce avoidable workload and improve the quality and resilience of services.

SDEG will not adopt technology because it is new. Adoption must demonstrate a meaningful contribution to Excellence. Differently., be proportionate to risk and preserve the human relationships, professional expertise and personal responsibility at the heart of excellent education.

The SDEG commitment
AI should augment people, not replace professional judgement; increase opportunity, not increase inequality; support learning, not obscure whether learning has taken place; and release time for human connection, creativity, expertise, service and community.

1.1 Strategic aims

- prepare pupils to understand, question and use AI confidently in further study, work and public life;
- help teachers and professional services staff focus more time on high-value human work;
- improve accessibility and inclusion without reducing ambition or independence;
- support thoughtful experimentation and shared professional learning;
- protect safeguarding, privacy, security, assessment integrity and public trust;
- evaluate impact honestly, including unintended effects and opportunity cost; and
- maintain a Group approach that enables local educational distinctiveness without fragmented governance.

1.2 Excellence. Differently. in practice

Dimension	What AI should enable
Excellence	High-quality teaching, critical thinking, secure services and well-informed decisions.
Differently	Creativity, responsible experimentation, accessible participation and new forms of learning.
Human flourishing	More time for relationships, reflection, feedback, mentoring, care and contribution.
Community	Shared knowledge, consistent safeguards and benefits that extend across the Group.

Future readiness	Pupils and staff able to understand capabilities, limitations, ethics and social implications.

AI and emerging technologies create opportunities to enrich teaching, develop pupils' knowledge and skills, reduce avoidable workload, improve accessibility and strengthen services. AI and emerging technologies also create risks involving safeguarding, privacy, bias, misinformation, intellectual property, assessment integrity, security, dependency and loss of human judgement. This Policy establishes how SDEG will pursue opportunity responsibly.

It applies to generative AI, machine learning, automated or algorithmic systems, predictive tools, adaptive learning, synthetic media, AI-enabled search or assistants, bots, image, audio and video generation, automated transcription, biometric or emotion-related technologies, robotics and other emerging digital tools used for Group activity.

This Policy is non-contractual and operates with safeguarding, data protection, assessment, acceptable-use, procurement and professional-conduct requirements. Breach may be addressed through the relevant procedure.

2. Legislation and Regulatory Framework

- UK GDPR and Data Protection Act 2018;
- Equality Act 2010;
- Human Rights Act 1998;
- Copyright, Designs and Patents Act 1988;
- Computer Misuse Act 1990;
- Keeping Children Safe in Education 2026;
- DfE policy and support materials on generative AI in education;
- DfE guidance on generative AI and data protection in schools;
- ICO guidance and practical resources on AI and data protection;
- JCQ regulations and guidance on AI use in assessments;
- awarding-body and examination requirements; and
- applicable consumer, product-safety, employment, safeguarding and procurement obligations.

3. Roles and responsibilities

3.1 Group Board of Governors

- approves this Policy and holds the Chief Operating Officer to account;
- receives assurance on material uses, safeguarding, data, assessment integrity, incidents and benefits;
- ensures appropriate capability and resources; and
- retains oversight of high-impact or strategically significant adoption.

3.2 Chief Operating Officer

- owns the Group framework and acts as executive link for Group Digital Services;
- oversees the Director of Digital Services;
- ensures educational, safeguarding, data-protection, commercial and technical review is integrated;
- approves or escalates high-risk and Group-wide uses;
- ensures approved-use, risk and incident registers are maintained; and
- reports material risks and assurance to the Chief Executive Officer and Group Board.

3.3 Director of Digital Services

- leads technical due diligence, security, integration and supportability review;
- maintains the approved AI and emerging technology register;
- ensures tools use approved accounts, configurations and data controls;
- monitors technical risk, supplier change and service dependency;
- supports incident response and retirement; and
- advises the Chief Operating Officer, Heads, DSLs, DPO and AI Leads.

3.4 Heads

- own safe and effective educational implementation within the school;
- appoint or identify an AI Lead where appropriate;
- ensure curriculum, assessment and staff-development arrangements are clear;
- ensure pupils, staff and families understand permitted use;
- approve local pilots within delegated limits; and
- review educational impact and emerging concerns.

3.5 Designated Safeguarding Leads

- assess safeguarding implications, including generated content, manipulation, grooming, unsafe interaction and age limits;
- ensure AI-related concerns are included in training, curriculum, risk assessment and incident response;
- support tool approval and annual review;
- maintain safeguarding records and external referrals; and
- work with Digital Services on filtering, monitoring and technical limitations.

3.6 DPO and information owners

- advise on lawfulness, fairness, transparency, minimisation, rights and DPIAs;
- assess personal data, inferences, prompts, outputs, retention and international transfer;
- ensure privacy information and contracts are appropriate; and
- support breach and individual-rights response.

3.7 AI Leads and curriculum leaders

- lead age-appropriate AI literacy and pedagogical development;
- support staff to identify safe and effective use;
- provide guidance on prompting, verification, attribution and design;
- gather evidence of benefit and unintended effects;
- share approved practice and escalate concerns; and
- avoid becoming the sole approver for data, safeguarding or technical risk.

3.8 Staff and governors

- use only approved tools and permitted data;
- apply professional judgement and verify outputs;
- be transparent where required;
- protect confidentiality, copyright and assessment integrity;
- report errors, bias, unsafe outputs, data loss and concerns; and
- remain accountable for final work and decisions.

3.9 Pupils

Pupils must follow teacher instructions, age restrictions, acceptable-use rules and assessment requirements. Pupils must protect personal information, acknowledge permitted AI use, submit their own work, verify information and report harmful, misleading or inappropriate content.

4. AI and emerging technologies framework

4.1 Policy statement

SDEG will support thoughtful experimentation and evidence-informed adoption where AI can improve education or services. AI will assist, not displace, professional responsibility. Users remain accountable for decisions and outputs. High-impact decisions about people will not be made solely by AI. Unapproved tools must not be used with Group personal, confidential or safeguarding information.

Pupils will be educated to understand AI's capabilities, limits, risks and social implications, and to use AI in ways that preserve learning, authorship and academic integrity.

4.2 Core principles

Principle	Application
Human responsibility	A named person remains responsible for purpose, use, review and outcome.
Safe by design	Safeguarding, privacy, security and foreseeable misuse are assessed before use.
Educational purpose	Use should strengthen learning, inclusion, creativity, feedback or staff capacity.

Evidence and proportionality	Adoption reflects benefit, risk, maturity, cost and available alternatives.
Transparency	People are told when AI materially shapes content, interaction or decisions.
Fairness and inclusion	Bias, accessibility and differential impact are considered and tested.
Data minimisation	Only necessary and authorised information is used.
Accuracy and verification	Outputs are checked against reliable sources and professional judgement.
Authorship and integrity	AI does not obscure who created work or whether learning outcomes were met.
Contestability	Affected people can question significant outputs and receive human review.
Reversibility	Pilots and changes have limits, exit arrangements and the ability to stop.
Continuous learning	Incidents, user feedback and evidence shape future decisions.

4.3 Approval and lifecycle

No AI or emerging technology may be adopted for Group activity merely because it is publicly available or embedded in another service. Approval is proportionate to risk and uses the following lifecycle: propose, assess, approve, pilot, deploy, monitor, review and retire.

Assessment domain	Minimum question
Purpose and benefit	Problem, users, educational or operational outcome, evidence and alternatives
Safeguarding	Age, interaction, generated content, misuse, vulnerable users and reporting
Data protection	Data types, lawful basis, DPIA, supplier use, retention, transfers and rights
Security	Accounts, access, logging, integration, model/data exposure and incident handling
Fairness and accessibility	Bias, representativeness, protected groups, language, SEND and adjustments

Human oversight	Named owner, competence, verification, intervention and appeal.
Assessment integrity	Permitted use, authenticity, attribution and malpractice controls.
Intellectual property	Inputs, training rights, ownership, licensing, attribution and output risk.
Supplier and resilience	Terms, changes, support, availability, dependency, exit and deletion.
Evaluation	Success measures, pilot limits, feedback, review date and stopping criteria.

4.4 Approved uses and prohibitions

The approved AI register will define tool, users, purpose, permitted information, conditions, review date and owner. Approval of a tool does not mean every use is approved.

8.1 Examples of potentially permitted use

- idea generation and drafting from non-sensitive information;
- lesson-resource development with professional verification;
- question, quiz or retrieval-practice generation;
- summarisation of authorised content where confidentiality is protected;
- accessibility, translation or format support with human review;
- analysis of appropriately prepared, lawful and authorised data;
- administrative drafting and workload support; and
- pupil use explicitly designed and supervised to meet a learning objective.

8.2 Prohibited or specially controlled use

- uploading personal, special-category, safeguarding, confidential or commercially sensitive information to an unapproved tool;
- solely automated decisions about admission, recruitment, grading, discipline, pastoral intervention, allocation of opportunity or other significant action;
- generation or sharing of harmful, abusive, discriminatory, deceptive, explicit or unlawful content;
- impersonation, deepfakes, manipulation or fabricated evidence;
- unacknowledged AI use where authorship, assessment or professional transparency requires disclosure;
- use that breaches age restrictions, supplier terms, copyright or assessment rules;
- reliance on outputs without suitable verification; and
- deployment of unapproved bots, integrations, agents or automated actions on Group systems.

4.5 Staff use

Staff may use AI to support planning, drafting, administration, analysis and professional learning where approved. Staff must select the appropriate tool and data, verify every material assertion, adapt output to the context, check bias and accessibility, protect confidential information and retain evidence where the use informs a significant decision or published output.

AI must not be used to outsource professional judgement, simulate consultation that did not occur, manufacture records, write references without factual verification, or create misleading impressions of personal authorship or evidence.

4.6 Pupil education and use

Every school will include age-appropriate AI literacy within its Digital Curriculum & Delivery Statement. Provision will address what AI is, how outputs are produced, limitations and hallucination, bias, privacy, intellectual property, environmental and social questions, manipulation, safe prompting, verification, attribution, assessment integrity and responsible participation.

Teachers will state whether AI is prohibited, permitted with conditions, required for a defined learning purpose or unrestricted within explicit boundaries. Expectations must be clear before work begins. Access and teaching must reflect age, maturity, SEND, vulnerability and applicable product terms.

4.7 Assessment, authorship and academic integrity

Work submitted for qualification assessment must be the pupil's own and comply with current JCQ and awarding-body requirements. Misuse of AI so that submitted work is not the pupil's own may constitute malpractice. Permitted AI-generated material must be acknowledged in the required manner and cannot substitute for evidence that the pupil independently met the assessment criteria.

- teachers establish suitable conditions and checkpoints for assessed work;
- pupils are taught what constitutes permitted use, acknowledgement and malpractice;
- teachers accept only work they reasonably consider authentic;
- concerns are investigated fairly under exams, assessment and malpractice procedures;
- AI-detection outputs are not treated as conclusive evidence on their own; and
- records are retained where required by examination or internal procedures.

4.8 Safeguarding

AI may contribute to grooming, coercion, harmful interaction, cyberbullying, extortion, generated or manipulated media, misinformation and exposure to inappropriate content. Safeguarding concerns must be reported to the DSL immediately and managed under the Child Protection and Safeguarding Policy. Staff must not unnecessarily copy or circulate harmful content.

4.9 Data protection, security and intellectual property

- do not input personal or confidential information unless the use is approved and lawful;
- complete a DPIA where processing is likely to create high risk;
- consider whether prompts and outputs are retained, reused for training or transferred internationally;
- provide appropriate transparency information;
- respect data-subject rights and avoid excessive inference or profiling;
- use secure accounts and approved integrations;
- verify sources and copyright status;
- do not assume AI output is accurate, original, unbiased or free to use; and
- record ownership, licensing, attribution and deletion requirements in supplier review.

4.10 Human oversight and significant decisions

AI may inform but must not solely determine a decision with significant educational, employment, safeguarding, admissions, financial, disciplinary or pastoral effect. The human decision-maker must understand the use and limitations of the system, consider relevant evidence, identify and correct error or bias, explain the decision appropriately and provide a route for human review.

4.11 Pilots, evaluation and innovation

Pilots must have a named owner, purpose, defined users, approved tool, risk assessment, duration, success measures, data rules, support, incident route and stopping criteria. A successful demonstration is not sufficient evidence for wider deployment. Evaluation will consider educational outcome, workload, inclusion, user experience, risk, cost and sustainability.

4.12 Training and capability

All staff receive foundational AI awareness covering safe use, data protection, safeguarding, verification, bias, intellectual property and assessment integrity. Additional development is provided for leaders, DSLs, AI Leads, teachers, assessors, professional services and technical staff according to role. Training will encourage professional curiosity without implying that all tools or uses are authorised.

4.13 Incidents, concerns and breaches

Issue	Required route
Safeguarding or harmful content	DSL immediately
Personal-data concern	DPO and Data Breach Procedure
Security, account or supplier concern	Digital Services immediately
Assessment authenticity or malpractice	Exams and assessment procedures

Staff conduct	Line manager and People Team
Bias, inaccuracy or unfair impact	AI Lead, Head and relevant specialist
Material policy or systemic concern	COO and Speaking Up route where appropriate

The Group may suspend a tool or use while risk is assessed. Incidents will be recorded, affected people supported, legal and external reporting considered, and learning translated into controls, curriculum, training or approval decisions.

4.14 Transitional arrangements

2026/27 transition
The governance, safeguarding, data-protection, assessment and acceptable-use requirements of this Policy apply to West Lodge from 1 September 2026. Tool availability and technical integration may differ until migration in September 2027 and must be documented in the approved-use register and West Lodge Digital Transition Plan.

- only approved locally available tools may be used;
- differences in accounts, filtering, monitoring, access or supplier terms must be assessed;
- personal or confidential information must not be moved into unapproved services;
- pupil curriculum and staff guidance must reflect actual local capability; and
- full alignment is confirmed through post-migration review.

4.15 Assurance and reporting

Assurance area	Minimum evidence
Approved use	Current register, owners, conditions and review dates
Safeguarding	Incidents, emerging risks, training and control effectiveness
Data protection	DPIAs, privacy information, breaches and supplier assurance
Education	Curriculum, pupil understanding, staff capability and learning impact
Assessment	Guidance, authenticity concerns, malpractice and staff practice
Fairness	Bias concerns, accessibility and differential impact

Benefits	Workload, service, inclusion or learning evidence
Suppliers	Change, dependency, security, terms and exit
West Lodge	Approved tools, local differences, risk and migration alignment

The Chief Operating Officer provides Group management assurance. Heads review school implementation and educational impact. Local School Boards receive local assurance. The Group Board receives an annual effectiveness review and prompt escalation of material risk or incident. Risk-led independent assurance is incorporated into the Annual Audit & Assurance Plan.

4.16 Controlled records

Record	Purpose
Approved AI and emerging technology register	Tool, owner, users, permitted purpose and data, conditions, review and status
AI risk and DPIA records	Safeguarding, privacy, security, fairness, assessment and mitigation
Pilot and evaluation record	Purpose, measures, findings, decision, limitations and next review
Incident and concern log	Issue, response, impact, referral, learning and closure
Training record	Foundational and role-specific completion and evaluation
Curriculum statement	Age-specific AI literacy and pupil-use expectations
Assessment guidance	Permitted use, attribution, authenticity and investigation procedures
West Lodge transition record	Local tools, differences, exceptions and alignment evidence

4.17 Implementation actions

Action	Owner	Timing	Evidence
Replace school AI policies with Group framework	COO and Heads	Following approval	Crosswalk and confirmed superseded content
Create approved AI register	Director of Digital Services	On adoption	Tool, purpose, data, conditions, owner and review
Create local AI curriculum statements	Heads and AI Leads	Before existing policies retire	Age-specific delivery and pupil expectations
Align assessment guidance	Heads, exams and assessment leads	Before assessed work cycle	JCQ-aligned staff and pupil materials
Staff training	COO, Heads and AI Leads	Induction and annual cycle	Completion and evaluation evidence
West Lodge local assessment	Head and Director of Digital Services	During 2026/27	Approved tools, differences, controls and migration actions

4.18 AI strategy, educational delivery and professional services

4.18.1 Group AI strategy

The Chief Operating Officer will maintain a proportionate Group AI strategy or implementation roadmap connecting educational priorities, professional-services opportunities, infrastructure, training, approved tools, safeguarding, risk, assurance and measurable benefit. The roadmap will distinguish exploration, pilot, approved deployment and retirement.

The strategy will not require every school or function to adopt the same educational use at the same time. It will require common governance, approved systems, clear ownership, evidence of benefit and transparent management of risk.

4.18.2 Progressive AI literacy

Phase	Minimum progression focus
Early Years / Pre-Prep	Trusted adults; simple distinction between people and technology; safe curiosity; asking for help; privacy and kind behaviour.

Prep	How AI answers questions or creates content; reliability; personal information; age restrictions; respectful and responsible use.
Junior	Prompting; checking sources; hallucination and misinformation; copyright; bias; safe use; acknowledgement and help-seeking.
Senior	Ethics; privacy; intellectual property; algorithmic influence; academic integrity; manipulation; evaluation of output and appropriate tool choice.
Sixth Form	Advanced verification and prompting; research practice; disciplinary and workplace applications; societal impact; accountability and independent authorship.

Each school will map these outcomes through its Digital Curriculum & Delivery Statement. The phase descriptors are minimum expectations rather than a prescribed scheme of work. Schools may exceed or sequence them differently where age, curriculum and pupil need justify this.

4.18.3 AI use categories for teaching and learning

Category	Teacher instruction
Prohibited	AI must not be used for the task. The work must be completed without AI assistance.
Permitted with conditions	Defined AI support may be used if the teacher's conditions, acknowledgement and evidence requirements are met.
Encouraged	AI use supports the learning objective and pupils are expected to explain, verify and evaluate its contribution.
Required	AI use is itself part of the learning objective and is taught, supervised and assessed accordingly.

Teachers must make the applicable category clear before work begins. Qualification assessments remain governed by JCQ, awarding-body and examination requirements, which take precedence over classroom categories.

4.18.4 Professional services

Function	Minimum control position
People	Drafting and process support may be permitted. AI must not solely determine recruitment, performance, disciplinary, grievance, remuneration or employment outcomes.
Finance	Analysis, forecasting and drafting may be permitted with approved data and human verification. AI must not authorise payments, override controls or make unsupported financial commitments.
Governance & Compliance	Research, drafting and information organisation may be permitted. AI must not replace legal advice, trustee judgement, formal assurance or authoritative records.
Admissions	Administrative support and communication may be permitted. AI must not solely select, rank or reject applicants or obscure published criteria and human review.
Marketing & Communications	Ideation and drafting may be permitted with factual, reputational, copyright and brand review. Synthetic media must not mislead.
Philanthropy and Commercial	Research and drafting may be permitted within approved data and relationship-management controls. Confidential donor, partner or commercial information requires authorised systems.
Estates and Operations	Planning, analysis and service support may be permitted. Safety-critical decisions require competent human assessment and established control processes.
Digital Services	Technical analysis, support and automation may be permitted within approved security, access, logging, testing and change controls.

4.19 Procurement and supplier standards

Before procurement, renewal or material expansion of an AI-enabled service, SDEG will complete proportionate due diligence. The level of evidence and approval must reflect pupil access, data sensitivity, autonomy, scale, criticality and potential impact.

- clear intended purpose, target users, age range, SEND considerations and evidence-supported claims;
- educational use case and evidence of benefit without exaggerated capability claims;
- filtering, monitoring and reporting capabilities where relevant;
- security, identity, access, logging, incident response and vulnerability arrangements;
- privacy, training-data position, prompt and output handling, retention, deletion and international transfers;
- intellectual-property terms for inputs, outputs, supplier training and generated material;
- testing for bias, accessibility, cognitive development, emotional and social development, mental health and manipulation;
- human oversight, user controls, transparency and routes to challenge or report;
- service levels, support, change notification, subcontractors, continuity, export and exit; and
- supplier assurance that product features remain suitable when materially modified.

Procurement rule
An approved supplier is not the same as an approved use. Every deployment must remain within the purpose, users, data, conditions and review date recorded in the Approved AI and Emerging Technology Register.

4.20 Impact, assurance and horizon scanning

Assurance domain	Evidence
Strategy and adoption	Roadmap progress, pilots, approved deployments, retirements and unresolved decisions.
Educational quality	Curriculum coverage, pupil literacy, teacher practice, inclusion, learning evidence and unintended effects.
Workload and service	Time released, service quality, user experience, duplication, cost and dependency.

Safeguarding	Incidents, generated or manipulated content, age restrictions, vulnerable users and control improvement.
Data protection and security	DPIAs, supplier assurance, access, incidents, retention and technical exceptions.
Assessment integrity	Guidance, pupil understanding, authenticity concerns, malpractice and staff confidence.
Fairness and accessibility	Bias concerns, reasonable adjustments, differential impact and challenge routes.
Capability	Training completion, professional confidence, community of practice and support demand.
Innovation pipeline	Emerging tools, evidence, proposed pilots, regulatory change and horizon risks.
West Lodge	Local tools, transition controls, migration readiness and alignment.

The annual effectiveness review will consider both control operation and realised benefit. Numbers of tools or users are not, by themselves, evidence of educational or organisational value. Material risks, incidents and overdue actions will be connected to the Group Risk Register and Annual Audit & Assurance Plan.

4.21 Excellence. Differently. and the future

SDEG does not view AI as a replacement for teachers, leaders, professional services staff or human relationships. Exceptional education remains profoundly human. The purpose of AI within SDEG is to enable people to flourish more fully through creativity, wisdom, expertise, service and community.

Used well, AI can help staff focus on the work that most needs professional judgement and human connection, and can help pupils develop the discernment required for a changing world. Used poorly, AI can undermine learning, trust, fairness and safety. SDEG will therefore remain ambitious about opportunity and disciplined about responsibility.

Our final test
Does this use help SDEG deliver Excellence. Differently. while remaining safe, effective, responsible, transparent and humanly accountable? If not, it should not proceed.

5. Monitoring

This policy will be reviewed annually by the Chief Operating Officer or sooner where required due to:

- legislative change;
- regulatory change;
- safeguarding developments;
- assessment or qualification changes;
- organisational change;
- a serious incident or breach;
- significant technology developments.

Monitoring and assurance activity will include approved AI register reviews, safeguarding audits, training compliance, DPIA reviews, assessment integrity monitoring, supplier assurance and incident analysis.

At every review, the policy will be approved by the Group Board of Governors.

6. Links with other policies

- Digital Services, Information Security & Cyber Resilience Policy;
- Digital Safeguarding & Online Safety Policy;
- Digital Communications & Acceptable Use Policy;
- Data Protection and Data Breach policies;
- Child Protection and Safeguarding Policies;
- Assessment, Exams, Academic Integrity and Malpractice policies;
- Staff Code of Conduct and pupil behaviour policies;
- Recruitment and Admissions policies;
- School Digital Curriculum & Delivery Statements; and
- West Lodge Digital Transition Plan.

Appendix 1: Approved AI and Emerging Technology Register

Register field	Required record
Product and version	Supplier, product, embedded AI feature and current version.
Purpose and owner	Approved problem/use case and named accountable owner.
Approved users	Staff roles, pupil phases, governors, suppliers or other authorised users.
Approved data	Information categories permitted and expressly prohibited.
Safeguarding status	Age range, pupil access, risk assessment, controls and DSL review.
Data protection status	Lawful basis, DPIA, privacy information, retention and DPO review.
Technical status	Identity, access, integration, logging, security review and support.
Educational / operational conditions	Tasks permitted, human checks, attribution and local restrictions.
Assessment position	Whether and how use is permitted in assessed work.
Supplier evidence	Product safety, terms, data use, copyright, change and exit.
Decision and dates	Approver, approval date, review date, pilot/approved/suspended/retired status.
Evidence and incidents	Evaluation record, material concerns, changes and decision history.

Appendix 2: AI impact assessment and approval form

Assessment field	Required information
Proposal	Tool, feature, use case, users and desired outcome.
Alternatives	Non-AI options and reason AI is proportionate.
Benefit hypothesis	What will improve, for whom, and how it will be measured.
Safeguarding	Age, vulnerability, contact/content/conduct risks and controls.
Data and privacy	Inputs, outputs, lawful basis, DPIA, retention and supplier use.
Security and resilience	Accounts, access, integration, logging, compromise, continuity and exit.
Fairness and inclusion	Bias, language, accessibility, SEND, protected groups and adjustments.
Human oversight	Named competent reviewer, intervention and challenge route.
Assessment and authorship	Rules, acknowledgement, authenticity and record requirements.
Intellectual property	Rights in inputs and outputs, attribution, licensing and publication.
Pilot design	Scope, duration, cohort, training, measures and stopping criteria.
Decision	Approve, approve with conditions, pilot, defer, reject, suspend or retire.
Review	Owner, date, evidence required and closure or renewal decision.

Appendix 3: Staff AI use aide-memoire

- ☐ Use an approved tool for an approved purpose.
- ☐ Do not enter personal, safeguarding, confidential or commercially sensitive information unless expressly authorised.
- ☐ Check facts, sources, calculations, tone, bias, accessibility and copyright.
- ☐ Adapt outputs using professional expertise rather than forwarding raw output.
- ☐ Keep meaningful human oversight over every significant decision.
- ☐ Be transparent about AI assistance where the context, assessment or policy requires it.
- ☐ Preserve evidence where AI materially informs a decision, assessment or published output.
- ☐ Report harmful output, data loss, bias, security concerns or unexpected behaviour.
- ☐ Stop and seek advice whenever safe, effective, responsible or humanly accountable use is unclear.

Appendix 4: AI use decision record (short form)

Field	Required information
Purpose	What problem or opportunity is being addressed?
Owner and users	Who is accountable and who will use it?
Tool and supplier	What system, version and terms apply?
Data	What information will be entered, generated, retained or shared?
Safeguarding	What risks, age limits and misuse scenarios apply?
Human oversight	Who verifies outputs and makes decisions?
Fairness and accessibility	How will bias and differential impact be addressed?
Assessment and authorship	What are the rules for pupil work and attribution?
Security and resilience	Access, integration, logging, support, dependency and exit.
Approval and review	Decision, conditions, date, reviewer and next review.

The SDEG AI test
Safe? Effective? Responsible? Transparent? Humanly accountable? If any answer is unclear, pause and seek advice.