SPORTING CHANCES GROUP

SCG ARTIFICIAL INTELLIGENCE (AI) USE, SAFETY & SECURITY FRAMEWORK

Lead	**David Johnson**
Last Reviewed	**November-2026**
Next Review Date	**November-2027**

This framework is to be reviewed **annually** and applies to **all** SCG provisions.

Version modified on 6 November 2026.

1. PURPOSE

Artificial Intelligence (AI), including generative AI, is increasingly being used across education, business, communications and everyday digital services.

Sporting Chances Group (SCG) recognises that AI can provide useful opportunities to support teaching, learning, accessibility, administration, communications, creativity and business operations. However, AI can also introduce safeguarding, data protection, cybersecurity, intellectual property, accuracy and professional conduct risks.

The purpose of this framework is to establish a clear and proportionate approach to the safe, responsible and secure use of AI across SCG.

This framework should be read alongside SCG's:

- Child Protection & Safeguarding Policy;
- Data Protection Policy;
- Staff Conduct Policy;
- Staff Handbook;
- Social Media, Digital Safeguarding & Media Use Policy; and
- relevant staff and student guidance.

The framework does not replace these policies. Instead, it provides a common set of principles and practical requirements for the use of AI.

SCG will review its approach as AI technology, legislation, guidance and safeguarding risks develop.

2. SCOPE

This framework applies to:

- all SCG employees;
- volunteers, contractors, consultants and agency workers where they use SCG systems or information;
- all SCG provisions and services;
- AI tools accessed using SCG equipment, accounts or information;
- AI tools used for SCG business or educational purposes, including where accessed from a personal device; and
- where applicable, pupils and young people using AI as part of SCG activities.

It applies to both **generative AI** and other AI-enabled technologies.

Examples include:

- chatbots and AI assistants;

- text-generation tools;
- image-generation and image-editing tools;
- AI video and audio generation;
- transcription and summarisation tools;
- AI-powered educational platforms;
- automated assessment or analysis tools;
- AI features built into Microsoft 365 or other software;
- AI-enabled recruitment, administration or communication tools; and
- AI systems capable of profiling, recommendation or automated decision-making.

3. WHAT DO WE MEAN BY AI?

For the purposes of this framework, **Artificial Intelligence (AI)** means technology capable of performing tasks that would ordinarily require human judgement or intelligence.

Generative AI refers to AI systems that can create new content, such as text, images, audio, video or computer code, in response to instructions or prompts.

AI is not necessarily a standalone application. AI functionality may be incorporated into software or services that SCG already uses.

Staff should therefore consider whether a tool they are using contains AI functionality even where the product itself is not primarily marketed as an AI service.

4. SCG'S APPROACH TO AI

SCG supports the **safe and purposeful use of AI**, where it provides a genuine benefit and its risks can be appropriately managed.

AI should:

1. have a clear and legitimate purpose;
2. be proportionate to the task;
3. protect children, young people and staff;
4. protect personal and confidential information;
5. comply with data protection requirements;
6. be used with appropriate human oversight;
7. not replace professional judgement;
8. be appropriately secure;
9. respect intellectual property and copyright;
10. be suitable for the age and needs of any young person using it; and

11. be approved where required before being introduced into SCG activities or systems.

AI should be treated as a **tool to support professional work, not as a replacement for professional responsibility**.

The DfE states that staff remain responsible for the appropriateness and accuracy of material produced using AI and that AI cannot replace human judgement and expertise.

5. PERMITTED STAFF USE OF AI

Subject to the requirements of this framework, staff may use approved AI tools to support appropriate professional activities.

Examples may include:

Teaching & Learning

- generating lesson or activity ideas;
- creating quizzes or educational resources;
- adapting materials for different levels of ability;
- creating accessible or alternative versions of resources;
- brainstorming examples or discussion topics;
- generating fictional scenarios;
- supporting creative activities; and
- developing ideas for vocational or enrichment activities.

Administration

- drafting agendas;
- structuring meeting notes;
- creating templates;
- summarising non-confidential information;
- brainstorming administrative processes;
- creating generic communications;
- organising information; and
- supporting routine business tasks.

Communications & Creative Work

- brainstorming social media ideas;
- generating first drafts of non-sensitive copy;
- developing creative concepts;

- generating or editing suitable illustrative imagery;
- developing design concepts; and
- supporting website or marketing content.

Any final material must be checked and approved by the responsible member of staff before being issued, published or relied upon.

6. HUMAN OVERSIGHT & PROFESSIONAL RESPONSIBILITY

AI-generated information may be inaccurate, incomplete, biased, misleading or entirely fabricated.

Staff must therefore:

- check AI-generated information before relying upon it;
- verify important factual claims against reliable sources;
- consider whether generated material is appropriate for its intended audience;
- check that communications accurately represent SCG;
- review AI-generated educational material for suitability and accuracy;
- ensure that safeguarding-related information is not generated or interpreted solely by AI; and
- apply their own professional judgement.

AI must not be treated as an authoritative source simply because its output appears confident, detailed or professional.

The member of staff using AI remains responsible for the final work.

7. PROHIBITED OR RESTRICTED USES

Staff must not use AI to:

- make significant decisions about a child, young person or member of staff without appropriate human assessment and oversight;
- generate or assess safeguarding decisions without professional judgement;
- create misleading or deceptive information about an individual;
- impersonate a pupil, parent/carer, colleague or other individual;
- generate abusive, discriminatory, threatening or harmful content;
- create sexualised content involving children or young people;
- create, request or distribute intimate or sexually explicit images of a child or young person;
- create or distribute deepfakes or other synthetic media intended to harm, humiliate, exploit or deceive;
- circumvent SCG's filtering, monitoring, security or access controls;
- attempt to bypass an AI service's safety controls for harmful purposes;

- upload confidential SCG information to an unapproved AI service;
- connect an unapproved AI service to SCG Microsoft 365, SharePoint, OneDrive, Teams, email or other systems;
- use AI to conceal misconduct or falsify records; or
- undertake any activity through AI that would otherwise breach SCG policy, safeguarding requirements or the law.

8. PERSONAL DATA AND CONFIDENTIAL INFORMATION

SCG staff must **not enter, upload, copy, paste or otherwise submit personal data into an AI tool unless the tool has been specifically approved by SCG for that purpose**.

This includes:

- pupil names or identifiable information;
- contact details;
- safeguarding information;
- behavioural or pastoral information;
- attendance information;
- SEND information;
- medical or health information;
- photographs, videos or identifiable images;
- staff personal data;
- assessment or academic information;
- incident information; and
- any other information which could identify an individual.

Staff should assume that information entered into a publicly available AI tool may be processed, retained or otherwise used by the provider unless SCG has established otherwise.

Where possible, staff should use:

- anonymised information;
- pseudonymised information;
- fictional examples; or
- information that contains no personal data.

SCG's Data Protection Policy must always be followed.

The DfE recommends that personal data is not used in generative AI tools and states that where its use is strictly necessary, appropriate data-protection measures must be in place.

9. SPECIAL CATEGORY AND SAFEGUARDING INFORMATION

Special category personal data requires additional protection.

Staff must **never enter special category personal data or safeguarding information into a publicly available or unapproved AI tool**.

This includes information relating to:

- health;
- disability or SEND;
- racial or ethnic origin;
- religious or philosophical beliefs;
- sexual orientation;
- biometric information;
- safeguarding concerns;
- abuse or neglect;
- mental health;
- family circumstances; or
- other highly sensitive information.

Where there is a legitimate and approved reason for an AI system to process such information, the processing must have been assessed and approved through SCG's data protection procedures.

10. APPROVED AI TOOLS

SCG will maintain an **Approved AI Tool Register**.

The register should identify:

AI Tool	Purpose	Approved Users	Personal Data Permitted?	Pupil Use?	Approval Date	Review Date
e.g. Microsoft CoPilot	e.g. Copy Writing	e.g. SCG email holders	Yes/No	Yes/No	[Date]	[Date]

Staff must only use AI tools for SCG purposes where:

- the tool has been approved where approval is required;
- its intended purpose is understood;
- relevant terms and age restrictions have been considered;
- data protection requirements have been assessed;
- appropriate security measures are in place; and
- any required contractual or DPIA requirements have been completed.

SCG may restrict or withdraw approval for an AI tool if its risks, functionality, supplier arrangements or data practices change.

11. AI TOOL APPROVAL PROCESS

Before introducing a new AI tool for SCG use, the person proposing the tool should consider:

Purpose

- What problem does the tool solve?
- Is AI necessary to achieve the intended purpose?
- Is there a safer or simpler alternative?

Data

- What information will be entered?
- Does the tool process personal data?
- Could the information identify a child, young person or member of staff?
- Is special category data involved?
- Is the information retained?
- Is it used to train or improve the AI model?

Security

- How are accounts protected?
- Is multi-factor authentication available?
- What permissions does the tool require?
- Does it integrate with Microsoft 365, SharePoint, OneDrive, Teams or other SCG systems?
- Can administrators control user access?

Safeguarding

- Can children access the tool?
- What age restrictions apply?
- Does it have appropriate safety controls?
- Can users generate harmful content?
- Does it involve direct conversational interaction with young people?
- Does it collect or retain information about young users?

Intellectual property

- Who owns the material submitted to the tool?
- Can the provider use submitted material to train its models?
- Could SCG, staff or pupil-created work be used without appropriate permission?

Compliance

- Has the DPO been consulted where required?
- Is a DPIA required?
- Is a Data Processing Agreement required?
- Are international data transfers involved?
- Has the tool been added to the relevant SCG register?

The DfE's product safety standards recommend considering intended use, permissions, authentication, security, privacy, intellectual property and child safety when assessing AI products for educational use.

12. "SHADOW AI"

SCG does not permit **shadow AI**.

Shadow AI means the use of AI tools or AI-enabled services for SCG work without the knowledge or approval of the appropriate SCG lead.

Staff must not:

- create unapproved AI accounts for SCG work;
- upload SCG documents to personal AI accounts;
- connect personal AI accounts to SCG systems;
- use browser extensions or AI assistants that can access SCG information without approval;
- copy confidential information into consumer AI tools; or
- use an AI service simply because it is free or readily available.

If a member of staff believes an AI tool could provide a useful benefit to SCG, they should request that it is assessed rather than using it informally.

13. AI & MICROSOFT 365 / SCG SYSTEMS

AI functionality may increasingly be built into software already used by SCG.

The presence of an AI feature within an existing SCG service does not automatically mean that it is approved for every purpose.

Before enabling or using an AI feature that can access SCG information, the relevant lead should consider:

- what information the AI can access;
- what permissions it has;
- whether it can access pupil or safeguarding information;
- how information is processed;
- whether information is retained;
- whether outputs are shared externally;
- whether the feature changes existing data-processing arrangements; and
- whether additional DPO or IT approval is required.

Access should be limited to the information necessary for the intended purpose.

14. AI & CHILDREN / YOUNG PEOPLE

SCG recognises that children and young people may encounter AI independently outside of SCG.

Where AI is used directly as part of an SCG activity, staff must consider:

- age restrictions;
- the young person's individual needs;
- SEND and accessibility considerations;
- safeguarding risks;
- the type of interaction the AI provides;
- whether conversations are retained;
- what personal information may be collected;
- whether appropriate filtering and monitoring are available;
- whether the young person understands the limitations of AI; and
- whether appropriate adult supervision is required.

Pupil-facing AI should only be introduced where SCG has determined that its educational benefit outweighs the associated risks.

Young people should be taught, where appropriate, that AI can:

- provide inaccurate information;
- generate convincing misinformation;
- produce inappropriate or harmful material;
- imitate people;
- create manipulated images, audio or video;

- facilitate scams or manipulation; and
- create content that may appear genuine when it is not.

AI literacy should form part of SCG's wider online-safety education.

15. AI, DEEPFAKES & SYNTHETIC MEDIA

AI can be used to create realistic but fabricated images, videos, audio recordings and conversations.

SCG treats the malicious creation or distribution of synthetic media involving pupils, young people or staff as a potential safeguarding concern.

Particular concern should be given to:

- deepfake images or videos;
- AI-generated intimate images;
- manipulated photographs;
- impersonation;
- fabricated messages or communications;
- AI-generated bullying;
- sexualised or humiliating synthetic content;
- content intended to blackmail or threaten an individual; and
- content intended to damage a person's reputation.

Staff must not create, request, share or distribute harmful synthetic media involving children or young people.

Where a member of staff becomes aware of potentially harmful AI-generated or manipulated content involving a pupil or young person, this must be reported through SCG's safeguarding procedures.

Staff should **not forward, download or redistribute potentially illegal or harmful material unnecessarily**.

KCSIE 2026 explicitly recognises AI-generated content within online-safety and safeguarding risks, including AI-generated intimate images. This should therefore be treated as part of SCG's existing safeguarding framework rather than as a separate category of harm.

16. AI & ONLINE SAFETY

AI-related risks should be considered within SCG's existing **4Cs online-safety framework**, in line with KCSIE 2026:

Content

AI may generate or amplify harmful, illegal, discriminatory, sexual, extremist, misleading or otherwise inappropriate content.

Contact

AI-powered chatbots and simulated interactions can create risks around manipulation, grooming, emotional dependence, inappropriate communication and disclosure of personal information.

Conduct

AI may be used for bullying, impersonation, harassment, creation of deepfakes, manipulation of images or other harmful behaviour.

Commerce

AI may facilitate scams, phishing, fraud, misleading advertising or other financial harms.

AI should therefore **not be treated as a fifth "C"**. It is a technology that can increase or change existing online-safety risks across all four areas.

17. AI & INTELLECTUAL PROPERTY

AI use must respect copyright and other intellectual property rights.

Staff must consider whether they have permission to upload or reproduce:

- pupil work;
- staff-created work;
- copyrighted images;
- photographs;
- educational resources;
- published materials;
- third-party documents; or
- other creative works.

Pupil and staff work should not be submitted to an AI system where doing so would result in inappropriate use, retention, commercial exploitation or training of AI models without the necessary permission.

Data protection permission and intellectual property permission are **separate considerations**. Permission to process personal data does not automatically give permission to use someone's creative work.

The DfE specifically distinguishes data-protection and intellectual-property considerations when using pupil or staff work with generative AI.

18. AI-GENERATED COMMUNICATIONS

AI may be used to assist with drafting communications, but staff remain responsible for the final communication.

AI-generated communications must be checked for:

- accuracy;
- tone;
- unintended implications;
- discriminatory or inappropriate language;
- confidentiality;
- safeguarding concerns;
- factual errors; and
- whether the communication accurately reflects SCG's position.

AI must not independently send communications to pupils, parents/carers, schools, local authorities or other external parties unless the system and use have been specifically approved for that purpose.

19. AI AND AUTOMATED DECISION-MAKING

SCG will exercise particular caution where AI could influence decisions about individuals.

AI must not be used as the sole basis for decisions relating to:

- safeguarding;
- pupil placement;
- behaviour;
- SEND;
- educational progress;
- disciplinary action;
- recruitment;
- staff performance;
- complaints; or
- other decisions that could significantly affect an individual.

Where AI is used to assist with analysis or decision-making, an appropriately qualified member of staff must retain responsibility for reviewing the information and making the final decision.

Any proposed use involving automated decision-making or profiling must be referred to the DPO before implementation.

20. CYBERSECURITY

AI tools must be treated as part of SCG's wider information-security environment.

Where applicable, AI systems should use:

- strong authentication;
- multi-factor authentication;
- appropriate role-based permissions;
- secure passwords;
- administrator controls;
- current software and security updates;
- appropriate access restrictions; and
- monitoring appropriate to the service and level of risk.

Staff must not attempt to circumvent security controls or use AI tools to gain unauthorised access to systems or information.

AI must not be used to create malware, conduct unauthorised security testing, obtain credentials, bypass access controls or undertake other activity that could compromise SCG systems.

The DfE's AI product-safety standards specifically identify authentication, permissions, security updates and compatibility with school/college cybersecurity standards as relevant safeguards.

21. AI-RELATED INCIDENTS

An AI-related incident should be reported where, for example:

- personal data has been entered into an unapproved AI service;
- confidential information has been disclosed to an AI provider;
- an AI tool has produced or distributed harmful content involving a pupil;
- a deepfake or manipulated image involving a pupil or staff member has been discovered;
- an AI system appears to have retained or exposed SCG information unexpectedly;
- an AI account has been compromised;
- an AI system has been used to bypass SCG security controls;
- an AI-generated communication has caused significant harm or risk; or
- staff become aware of another significant misuse of AI.

Reporting route

Data protection / information security:

Report immediately to: **Data Protection Officer**

Safeguarding:

Report immediately to the **Designated Safeguarding Lead (DSL)** or appropriate safeguarding lead.

IT / cybersecurity:

Report to **IT Lead / IT provider**

Staff should report concerns promptly even where they are unsure whether an incident constitutes a formal breach.

22. STAFF TRAINING & AWARENESS

All relevant staff will receive appropriate AI awareness training.

Training should cover, as appropriate:

- what AI and generative AI are;
- appropriate and inappropriate uses;
- AI accuracy and hallucinations;
- safeguarding risks;
- deepfakes and synthetic media;
- AI-generated intimate images;
- grooming, manipulation and emotional dependence;
- misinformation and bias;
- data protection;
- confidentiality;
- cybersecurity;
- intellectual property;
- approved SCG AI tools;
- reporting procedures; and
- professional responsibility.

SCG should use the DfE's **Safe use of generative AI in education: Module 3** as a key resource for staff awareness training. The DfE recommends that all education staff complete this module, which covers safeguarding, ethics, data and intellectual property.

AI awareness should be refreshed as part of SCG's wider annual safeguarding, online-safety and data-protection training.

23. STAFF RESPONSIBILITIES

All staff are responsible for:

- following this framework;
- using only appropriate and approved AI tools;
- protecting SCG and individual data;
- checking AI-generated content;
- applying professional judgement;
- reporting concerns and incidents;
- respecting copyright and intellectual property;
- completing required training; and
- asking for advice where they are unsure.

Staff should never assume that an AI tool is safe simply because it is widely used or freely available.

24. MANAGEMENT RESPONSIBILITIES

SCG leadership and relevant policy owners are responsible for:

- maintaining an appropriate AI governance framework;
- identifying approved AI tools;
- ensuring appropriate staff training;
- considering AI within safeguarding risk assessments;
- ensuring AI use is consistent with data protection requirements;
- reviewing significant AI-related incidents;
- ensuring appropriate security controls;
- considering AI when procuring new digital services; and
- reviewing this framework regularly.

The DPO, DSL and IT/digital lead should work together where AI presents overlapping **data protection, safeguarding and cybersecurity risks**.

25. PROCUREMENT AND SUPPLIER DUE DILIGENCE

Where SCG is considering procuring an AI-enabled service, the responsible person should establish, as appropriate:

- the supplier and ownership of the service;
- intended purpose and educational use case;
- age restrictions;
- data collected;
- data storage location;
- international transfers;
- retention arrangements;
- whether data is used for model training;
- subprocessors;
- security measures;
- authentication and access controls;
- safeguarding features;
- filtering and monitoring;
- intellectual property arrangements;
- contractual terms;
- Data Processing Agreement requirements;
- DPIA requirements; and
- arrangements for deletion or return of SCG data when the service ends.

AI procurement should follow SCG's existing requirements for approved third-party processors and cloud services.

26. RECORD KEEPING

SCG should maintain appropriate records relating to significant AI systems and processing activities, including where relevant:

- Approved AI Tool Register;
- AI risk assessments;
- DPIAs;
- Data Processing Agreements;
- supplier information;
- approval decisions;
- staff training records;
- significant AI-related incidents; and
- annual reviews of AI use.

Where AI involves personal data, the processing should be reflected in SCG's existing data-processing documentation where required.

27. ANNUAL REVIEW

SCG will review its AI use and associated risks at least annually and sooner where significant changes occur.

The review should consider:

- new AI technologies;
- new AI functionality within existing SCG systems;
- safeguarding risks;
- data protection risks;
- cybersecurity risks;
- staff and pupil use;
- incidents and lessons learned;
- changes to legislation or regulatory guidance;
- supplier changes;
- changes to approved tools;
- staff training needs; and
- whether existing controls remain proportionate and effective.

AI risks should be considered as part of SCG's wider annual online-safety and safeguarding review.

28. QUICK REFERENCE: THE SCG AI RULES

Before using AI for SCG work, staff should remember:

STOP

S — Sensitive information

Don't put personal, confidential or safeguarding information into an unapproved AI tool.

T — Think

Ask whether AI is appropriate for the task and whether there is a safer alternative.

O — Officially approved

Use approved tools and follow SCG's requirements.

P — Professional judgement

Check the output. You remain responsible for the final result.

If in doubt:

Don't upload it. Don't connect it. Ask first.

Speak to the appropriate DPO, DSL or IT/digital lead before proceeding.

29. RELATED SCG POLICIES & PROCEDURES

This framework should be read alongside:

- SCG Child Protection & Safeguarding Policy;
- SCG Data Protection Policy;
- SCG Staff Conduct Policy;
- SCG Staff Handbook;
- SCG Social Media, Digital Safeguarding & Media Use Policy;
- SCG Data Retention Schedule; and
- SCG Data Protection Impact Assessment (DPIA) process.

30. REFERENCE MATERIAL

This framework should be reviewed against current Department for Education and other relevant official guidance, including:

- Keeping Children Safe in Education (KCSIE);
- DfE Generative AI in Education guidance;
- DfE Generative AI Product Safety Standards;
- DfE Safe Use of Generative AI in Education training materials;
- DfE Data Protection in Schools guidance;
- UK GDPR and Data Protection Act 2018;
- applicable UK data protection legislation and regulations; and
- relevant cybersecurity guidance.

SCG will update this framework where changes to legislation, statutory guidance or significant developments in AI technology require changes to its approach.

APPENDIX 1 — AI TOOL APPROVAL CHECKLIST

Proposed AI Tool: _____

Proposed by: _____

Date: _____

Purpose: _____

Purpose and suitability

☐ Is there a clear reason for using AI?

☐ Is the intended use appropriate for SCG?

☐ Is there a non-AI alternative?

☐ Is the tool appropriate for the intended users?

Data protection

☐ Will personal data be processed?

☐ Will special category data be processed?

☐ What data is collected?

☐ Where is it stored?

☐ Is data transferred internationally?

☐ Is data retained?

☐ Is data used for model training?

☐ Has the DPO been consulted?

☐ Is a DPIA required?

☐ Is a Data Processing Agreement required?

Safeguarding

☐ Is the tool child-facing?

☐ What age restrictions apply?

☐ What safeguarding controls exist?

☐ Can harmful content be generated?

☐ Can users interact directly with an AI chatbot?

☐ Are filtering and monitoring available?

Security

☐ Does the tool support MFA?

☐ Are role-based permissions available?

☐ What information can the tool access?

☐ Does it integrate with SCG systems?

☐ Can administrator access be controlled?

☐ Are security updates provided?

Intellectual property

☐ What happens to uploaded content?

☐ Can uploaded content be used for model training?

☐ Could pupil or staff work be affected?

☐ Are appropriate permissions in place?

Approval

DPO: _____ Date: _____

DSL / Safeguarding Lead (where applicable): _____ Date: _____

IT / Digital Lead: _____ Date: _____

Final approval: _____ Date: _____

Review date: _____

APPENDIX 2 — APPROVED AI TOOL REGISTER

Tool	Purpose	Staff Use	Pupil Use	Personal Data	Special Category Data	M365/SCG Integration	DPO Approval	Review
e.g. CoPilot	Writing emails	Yes/No	Yes/ No	Yes/No	Yes/No	Yes/No	[Date]	[Date]

APPENDIX 3 — AI INCIDENT RECORD

Date/time: _____

Reported by: _____

AI tool involved: _____

Type of incident:

☐ Personal data disclosure

☐ Safeguarding concern

☐ Deepfake / synthetic media

☐ Cybersecurity incident

☐ Inappropriate AI-generated content

☐ Intellectual property concern

☐ Unapproved AI use

☐ Other: _____

Brief description:

Information involved:

Immediate action taken:

Reported to:

☐ DPO

☐ DSL

☐ IT / cybersecurity lead

☐ Senior leadership

☐ Other: _____

Further action / lessons learned:

Date closed: _____

Reviewed by: _____