DIGITAL SAFEGUARDING & ONLINE SAFETY 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	Establishes the Group-wide framework for digital safeguarding, online safety, filtering, monitoring, curriculum delivery and assurance.

1. Aims

This Policy replaces duplicated safeguarding and online-safety provisions in school IT policies. Infrastructure, cyber-security and information-security requirements sit in the Group Digital Services, Information Security & Cyber Resilience Policy. Staff communications and acceptable use sit in the Group Digital Communications & Acceptable Use Policy. AI governance sits in the Group AI & Emerging Technologies Policy.

The safeguarding operating rule
Heads and DSLs own safeguarding judgement and response. The Chief Operating Officer provides executive oversight of Group Digital Services and oversees the Director of Digital Services. Digital Services provides technical controls and evidence, but safeguarding decisions are not delegated to the technical team.

SDEG recognises that technology is integral to learning, relationships, communication and daily life. Digital safeguarding is therefore part of safeguarding, not a separate technical activity. This Policy establishes how the Group will educate, protect, identify, respond, learn and assure online safety across all schools and nurseries.

The Policy applies to activity using Group networks, systems and devices and to conduct outside school where it affects a pupil, the safe operation of a school, the welfare of the community or a member of staff's professional responsibilities. It applies to pupils, staff, governors, volunteers, contractors, visitors and parents or carers where relevant.

This Policy does not replace the Child Protection and Safeguarding Policy. Any concern about a child must be managed through the safeguarding procedures, regardless of the technology, platform, device, location or time involved.

SDEG will provide a learning environment in which children and young people develop the knowledge, confidence and judgement to participate safely and responsibly online. The Group will maintain proportionate filtering and monitoring, clear reporting routes, age-appropriate education, trained staff, supportive responses and effective governance.

Online incidents will be considered in context. The Group will distinguish safeguarding need, behaviour, vulnerability, technical failure, criminal concern and educational opportunity. The welfare of the child remains central, including where a pupil has caused harm as well as where a pupil has experienced harm.

2. Legislation and Regulatory Framework

- Keeping Children Safe in Education 2026;
- Education (Independent School Standards) Regulations 2014;
- Early Years Foundation Stage statutory framework;
- Children Acts 1989 and 2004 and Working Together to Safeguard Children;
- Prevent duty guidance;
- Equality Act 2010;
- UK GDPR and Data Protection Act 2018;

- Education Act 1996 and Education and Inspections Act 2006;
- DfE Searching, Screening and Confiscation guidance;
- UKCIS guidance for education settings;
- DfE filtering and monitoring core standard, updated June 2026; and
- UK Safer Internet Centre appropriate filtering and monitoring definitions.

The Independent School Standards do not prescribe a policy with this title. This Policy supports compliance with safeguarding and welfare requirements and with the responsibility of leadership and management to ensure standards are met consistently.

3. Roles and responsibilities

3.1 Group Board of Governors

- approve this Policy and hold the Chief Operating Officer and Heads to account for implementation;
- ensure appropriate filtering and monitoring systems and an annual effectiveness review;
- receive assurance on curriculum, incidents, vulnerable pupils, emerging risk, technical limitations and actions;
- ensure adequate resources, capability and independent challenge; and
- require material safeguarding weaknesses to be addressed promptly.

3.2 Group assurance

- scrutinise the effectiveness of the Group framework;
- review themes, complaints, curriculum assurance, filtering and monitoring review outcomes and action status;
- seek assurance that age and setting differences are addressed; and
- escalate material concerns to the Group Board.

3.3 Safeguarding Link Governor

- meets appropriate leaders and review evidence without taking operational ownership;
- tests whether leadership, safeguarding and technical responsibilities are understood;
- reviews the annual filtering and monitoring effectiveness evidence;
- reports assurance and unresolved concerns to the Group Board; and
- maintains relevant safeguarding and online-safety knowledge.

3.4 Local School Boards

- receive local assurance on curriculum, pupil voice, incidents, vulnerable groups and improvement actions;
- support and challenge the Head; and
- escalate recurring or material issues through the agreed route.

3.5 Chief Operating Officer

- acts as executive link for Group Digital Services;
- oversees the work of the Director of Digital Services;
- ensures safeguarding and technical leaders work together;
- ensures systems, resources, suppliers, assurance and improvement activity support this Policy;
- resolves material cross-Group operating issues; and
- reports significant risks, incidents and assurance to the Chief Executive Officer and governance bodies.

3.6 Heads

- hold local accountability for implementation and pupil safety;
- nominate an SLT member responsible for filtering and monitoring;
- ensure age-appropriate curriculum and local delivery arrangements;
- ensure staff understand reporting and response duties;
- ensure behaviour, safeguarding and parental communication are aligned; and
- approve and review the school Digital Curriculum & Delivery Statement.

3.7 Designated Safeguarding Leads

- lead safeguarding assessment and response to online concerns;
- maintain understanding of filtering and monitoring capabilities, processes and limitations;
- support the annual effectiveness review and identify current safeguarding needs;
- ensure alerts and referrals are triaged, recorded and acted upon;
- ensure vulnerable pupils receive additional education or support;
- include online safety and emerging technology within safeguarding training and audit; and
- liaise with external agencies where required.

3.8 SLT member responsible for filtering and monitoring

- leads and documents the effectiveness review at least once each academic year;
- works with the DSL and Digital Services to identify current provision, gaps and needs;
- ensure checks cover relevant devices, locations, apps and remote use;
- considers whether controls address dynamic, personalised and AI-generated content;
- balances protection with access to legitimate teaching and learning; and
- reports findings and actions to the Head and governance route.

3.9 Director of Digital Services

- provides and maintains technically appropriate filtering and monitoring controls;
- documents coverage, configuration principles, tests, limitations and exceptions;
- supports the annual review and provide technical evidence;
- ensures mandatory illegal-content protections cannot be casually bypassed;

- maintains user attribution and alert-routing arrangements where technically appropriate;
- responds promptly to control failures and safeguarding escalation; and
- avoids making safeguarding judgements that belong to DSLs and school leaders.

3.10 Curriculum and digital-learning leads

- design a progressive and age-appropriate online-safety curriculum;
- map provision across curriculum, pastoral education, assemblies and wider school life;
- ensure staff have suitable materials and subject-specific guidance;
- include digital literacy, information reliability, privacy, AI and responsible participation; and
- evaluate impact through pupil work, discussion, feedback and incident themes.

3.11 Staff

- complete required training and maintain professional curiosity;
- teach and model safe, responsible digital behaviour;
- supervise use appropriately and follow local device expectations;
- report child concerns immediately through safeguarding routes;
- report filtering, monitoring or technical failures promptly;
- do not bypass controls except through an approved process; and
- respond to online child-on-child abuse with the same seriousness as offline harm.

3.12 Pupils and parents or carers

Pupils are expected to follow acceptable-use and behaviour expectations, protect personal information, treat others respectfully, use reporting routes and engage in online-safety education. Parents and carers are encouraged to engage with guidance, reinforce safe practice, report concerns and work with the school where support or action is needed.

4. Digital safeguarding and online safety framework

4.1 Online-safety framework

Risk domain	Examples considered by the Group
Content	Being exposed to illegal, harmful, misleading, discriminatory or age-inappropriate material, including AI-generated or manipulated material.
Contact	Harmful interaction, coercion, exploitation, grooming, harassment or unsafe contact with others.
Conduct	Personal online behaviour that increases risk or causes harm, including bullying,

	impersonation, non-consensual sharing, misuse of images or exclusion.
Commerce	Scams, fraud, gambling-like features, harmful advertising, privacy exploitation, unsafe purchases or financial pressure.
Technology and AI	Dynamic, personalised and generated content; unreliable outputs; unsafe bots; manipulated media; data misuse; algorithmic amplification and emerging tools.

Risk assessment will consider age, developmental stage, SEND, disability, vulnerability, language, family context, device ownership, remote access, platform design and the particular needs of the school community.

4.2 Core principles

Principle	Application
Safeguarding first	Online concerns are acted upon through the safeguarding framework.
Education plus protection	Technical controls support, but do not replace, curriculum, supervision and trusted relationships.
Age and need appropriate	Education, access and response reflect age, development, SEND and vulnerability.
Leadership-owned	Filtering and monitoring are not delegated solely to Digital Services or a supplier.
Proportionate	Controls and responses protect pupils without unreasonably restricting learning.
Listen and respond	Pupils know how to report and are taken seriously.
No shame in seeking help	Pupils are encouraged to report mistakes, unwanted contact, harmful content or pressure early.
Evidence-based	Reviews use incidents, pupil voice, curriculum evidence, technical tests and trend information.

Collaborative	Schools, families, safeguarding staff and technical staff share appropriate responsibility.
Continuously improving	Incidents, near misses and new technologies inform teaching, controls and policy.

4.3 Education and curriculum

Every school will maintain a concise Digital Curriculum & Delivery Statement showing how the Group outcomes below are taught progressively and how local age, curriculum and community needs are addressed. The statement is educational documentation, not a separate infrastructure or compliance policy.

Curriculum outcome	Minimum coverage
Safe access and privacy	Secure accounts and devices; personal information; permissions; location and image sharing; reporting loss or concern.
Relationships and behaviour	Respect, consent, boundaries, bullying, bystander action, reputation and help-seeking.
Content and media literacy	Reliability, misinformation, manipulation, recommender systems, advertising and source evaluation.
AI literacy	Capabilities, limits, bias, privacy, generated content, responsible use and recognition of manipulation.
Security and scams	Phishing, social engineering, fraud, malicious links and appropriate response.
Wellbeing and self-regulation	Healthy use, persuasive design, pressure, comparison, sleep and knowing when to seek support.
Law, rights and responsibility	Copyright, ownership, privacy, harmful or illegal behaviour and consequences.
Reporting and resilience	Trusted adults, school routes, platform tools, evidence preservation and recovery after an incident.

Schools may preserve and develop current age-specific curricula, including Pre-Prep, Prep, Junior, Senior and Sixth Form outcomes, through their local statement. No local statement

may dilute Group safeguarding expectations or reintroduce infrastructure and compliance ownership that this Tier 1 suite centralises.

4.4 Filtering and monitoring

4.4.1 Purpose

Filtering is preventative and limits access to illegal, inappropriate or potentially harmful content. Monitoring is reactive and helps identify activity that may indicate safeguarding need. Neither replaces staff supervision, curriculum, relationships, reporting or professional judgement.

4.4.2 Annual effectiveness review

A documented review must take place at least once in every academic year. It is led by the nominated SLT member responsible for filtering and monitoring, with the support of the DSL and Digital Services. Additional review is required after a material incident, system change, identified weakness or significant change in pupil need.

- current provision and known gaps;
- pupil and staff safeguarding needs;
- coverage of networks, managed devices, browsers, apps, embedded content and remote use;
- mobile and personally owned device risks;
- user identification and attribution;
- illegal-content protections and prevent-related requirements;
- dynamic, personalised, encrypted and AI-generated content;
- alert accuracy, capacity, triage, response and record keeping;
- supplier information and technical limitations;
- educational over-blocking and controlled exception routes;
- evidence from tests, incidents, pupil voice, DSL records and staff feedback; and
- actions, owners, due dates and verification.

4.4.3 Checks and evidence

Technical checks must be carried out on a risk-based schedule and after material configuration change. Records must identify what was checked, where, on which type of device or service, the result, issue found, immediate response, owner and closure evidence.

4.4.4 Bypass and exceptions

Users must not attempt to bypass filtering or monitoring. An educational or operational exception may be approved only where necessary, proportionate and safe. It must be controlled, time-limited where appropriate, documented and reviewable. Mandatory illegal-content protections must not be capable of ordinary user override.

4.5 Reporting and responding to concerns

A pupil or adult may report a concern to any trusted member of staff. Staff must listen, avoid blame, protect immediate safety, preserve relevant information where appropriate and report through the safeguarding route without delay. Technical teams may preserve logs or restrict access when instructed but must not delay safeguarding action.

Concern	Required route
Immediate danger or suspected crime	Protect the child, inform the DSL and use emergency or agency routes as required.
Child safeguarding concern	Record and manage under the Child Protection and Safeguarding Policy.
Child-on-child online harm	Consider needs and safety of all involved; manage under safeguarding and behaviour frameworks.
Cyberbullying or harassment	Safeguard, investigate proportionately and apply behaviour or anti-bullying arrangements.
Harmful or illegal content	Protect access, preserve necessary evidence, refer to DSL and consider reporting routes.
Account or device compromise	Notify Digital Services immediately and consider safeguarding and data-protection impact.
Filtering or monitoring failure	Notify Digital Services and DSL; apply interim controls and record remediation.
Data breach	Notify the DPO and follow the Data Breach Procedure.
AI-related concern	Apply safeguarding, behaviour, assessment, data and AI policy routes according to the issue.

Where behaviour may reflect vulnerability, coercion, exploitation, SEND need, distress or lack of understanding, response must include support as well as proportionate consequences. A sanction alone is not a safeguarding response.

4.6 Specific online-safety arrangements

4.6.1 Cyberbullying and harmful communication

Online bullying, harassment, threats, impersonation, exclusion or misuse of digital content will be addressed under safeguarding, anti-bullying and behaviour arrangements. The school will consider reach, repetition, audience, power imbalance, anonymity, permanence and impact.

4.6.2 Sharing and manipulation of images or media

Concerns involving images, recordings or digitally manipulated media must be reported immediately to the DSL. Staff must not copy or forward material unnecessarily. The DSL will determine safe handling, referral and support in line with current statutory and sector guidance.

4.6.3 Radicalisation, extremism and harmful influence

Online content and contact that may indicate radicalisation, extremist influence or other significant harm will be managed through safeguarding and Prevent arrangements. Filtering supports this duty but does not replace staff awareness or referral.

4.6.4 Generative AI and emerging technology

AI can create or amplify safeguarding risks through generated or manipulated content, misinformation, unsafe interactions, impersonation and privacy misuse. The AI & Emerging Technologies Policy governs approval and permitted use. This Policy governs safeguarding education, reporting and response.

4.6.5 Personal and mobile devices

Each school will set age-appropriate rules in its Digital Curriculum & Delivery Statement and pupil agreement. Rules will address when devices may be brought, stored or used; photography and recording; access to school systems; sanctions; safeguarding response; and reasonable adjustments. Technical and safeguarding limitations of mobile apps and personal connectivity must be considered in risk assessment.

4.6.6 Searching devices

Any search, examination, confiscation or deletion involving a pupil device must follow current statutory guidance, the school behaviour policy and safeguarding procedures. Staff must act within authority, protect privacy, avoid unnecessary access and consult the DSL where safeguarding content or risk is suspected.

4.6.7 Remote learning and off-site use

Schools will apply safeguarding expectations to school-provided devices, accounts, remote learning, educational visits and home access as far as reasonably practicable. Pupils and families will receive clear information about coverage, monitoring, privacy and reporting routes.

4.7 Vulnerable pupils and reasonable adjustments

- consider SEND, disability, communication, cognition, trauma, language, care experience and other vulnerability;
- adapt teaching, reporting routes and supervision;
- avoid removing access to beneficial technology without considering alternatives;
- involve parents or carers and specialists appropriately;
- review whether monitoring alerts or patterns indicate unmet need; and
- ensure reasonable adjustments do not create unmanaged safeguarding gaps.

4.8 Staff training and professional practice

All staff receive online-safety and digital-safeguarding training at induction and at least annual refreshers, with updates when risk, guidance or systems change. DSLs, Heads, the nominated SLT lead and relevant Digital Services staff receive role-specific development.

- the online element of safeguarding and child-on-child abuse;
- the Group reporting routes and local contacts;
- filtering and monitoring responsibilities and limitations;
- AI-generated and manipulated content;
- phishing, scams, privacy and data protection;
- age and SEND-informed response;
- professional boundaries and use of school systems; and
- how to respond without blame and preserve appropriate evidence.

4.9 Working with parents, carers and pupils

Schools will communicate expectations, curriculum, reporting routes, emerging risks and available support. Pupil voice will contribute to review of curriculum, controls and safe reporting. Parent engagement will be supportive, practical and age-appropriate, recognising that technology and family circumstances differ.

4.10 West Lodge transitional arrangements

Transitional status
West Lodge joins SDEG on 1 September 2026 but is not expected to complete technical migration to the Group digital operating model until September 2027. Safeguarding duties, leadership accountability, training, reporting and annual review requirements apply immediately. Approved local technical arrangements may continue during the transition.

- the Head must nominate the responsible SLT member and ensure the local framework is implemented;
- the DSL must understand and assure the local filtering and monitoring processes;
- existing local filtering, monitoring, device and reporting arrangements must be documented;
- the annual effectiveness review must test actual West Lodge coverage and limitations;
- gaps against Group expectations must be entered in the West Lodge Digital Transition Plan and Exception Register;
- interim safeguards must be assigned and reviewed; and
- migration must preserve safeguarding continuity before, during and after cutover.

4.11 Assurance, metrics and reporting

Assurance area	Minimum evidence
Leadership	Named roles, training, review meetings and action ownership.
Filtering and monitoring	Annual effectiveness review, technical checks, gaps, limitations and closure.
Curriculum	Mapped provision, staff confidence, pupil knowledge and age progression.
Incidents	Themes, severity, response, repeat patterns and learning.
Vulnerable pupils	Additional provision, reasonable adjustments and outcomes.
Pupil voice	Confidence in reporting, awareness of support and emerging experiences.
Parents and carers	Engagement, recurring questions, guidance and complaints.
Staff	Training, understanding, reporting and professional practice.
AI and emerging risk	New tools, generated content, manipulated media and response readiness.
West Lodge	Transition risks, interim safeguards, review evidence and migration readiness.

Heads review local effectiveness at least annually and report to Local School Boards. The Chief Operating Officer provides Group management assurance. The Group Board receives termly or proportionate reporting and an annual effectiveness review and prompt escalation of material concerns.

The Safeguarding Link Governor provides independent challenge and assurance. Material control failure, repeated concern or risk above tolerance is connected to the Group Risk Register and Annual Audit & Assurance Plan.

4.12 Controlled local documents and records

Controlled record	Purpose
School Digital Curriculum & Delivery Statement	Age-specific curriculum, local device rules, pupil agreements, reporting routes and named leads.
Filtering and monitoring effectiveness review	Leadership, safeguarding and technical evaluation at least annually.
Technical test record	Devices, locations, services, results, failures and remediation.
Online-safety incident record	Concern, assessment, action, referral, support, outcome and learning.
Curriculum map and evidence	Progression, delivery, assessment, pupil voice and review.
Training record	Induction, annual update, role-specific training and follow-up.
Exception record	Approved bypass, limitation or temporary safeguard, owner and expiry.
West Lodge transition record	Local provision, gaps, controls, milestones and closure evidence.

4.13 Implementation actions

Action	Owner	Timing	Evidence
Retire duplicated school IT policy provisions	Heads, DSLs and COO	Following approval	Crosswalk and confirmed superseded content.
Create school Digital Curriculum & Delivery Statements	Heads and curriculum/digital leads	Before local policies are retired	Age-specific delivery, device rules, pupil agreements and contacts.

Assign SLT filtering and monitoring leads	Heads	Before 1 September 2026	Named role, job description and training.
Complete annual effectiveness reviews	SLT lead, DSL and Digital Services	Once each academic year	Documented review and tracked actions.
West Lodge transition assurance	Head, DSL, COO and Director of Digital Services	Throughout 2026/27	Local baseline, review, exception record and migration safeguards.
Create Group assurance dashboard	COO with Heads and DSLs	For first annual assurance cycle	Consistent definitions, evidence and reporting.

5. Monitoring

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

- legislative change;
- safeguarding developments;
- regulatory change;
- inspection findings;
- organisational change;
- a significant incident;
- emerging technology risks.

Monitoring and assurance activity will include filtering and monitoring reviews, safeguarding incidents, pupil voice, curriculum assurance, training compliance, governance reporting and annual effectiveness reviews.

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

***6.* Links with other policies**

- Child Protection and Safeguarding Policies;
- Digital Services, Information Security & Cyber Resilience Policy;
- Digital Communications & Acceptable Use Policy;
- AI & Emerging Technologies Policy;
- Expected Pupil Behaviour and Anti-Bullying Policies;
- Staff Code of Conduct;
- Data Protection and Data Breach policies;
- Prevent and safeguarding procedures;
- Searching, Screening and Confiscation arrangements;

- School Digital Curriculum & Delivery Statements and pupil acceptable-use agreements; and
- West Lodge Digital Transition Plan and Exception Register.

Appendix 1: Annual filtering and monitoring effectiveness review

Review domain	Evidence required
Leadership	Named SLT lead, DSL, technical support and governance route.
Needs	Current pupils, vulnerable groups, staff, curriculum and local context.
Coverage	Networks, devices, browsers, apps, remote use and personal connectivity.
Filtering	Illegal and harmful content, dynamic/AI content, encrypted traffic and exceptions.
Monitoring	Strategy, user attribution, alert quality, triage, capacity, response and records.
Testing	Devices, locations, users, services, failures and retesting.
Education impact	Over-blocking, curriculum access, reasonable adjustments and support.
Incidents and voice	DSL records, technical events, pupil voice, staff and parent feedback.
Supplier assurance	Capabilities, limitations, changes, support and evidence.
Actions	Owner, priority, due date, interim safeguard and verified closure.

Appendix 2: Material escalation triggers

- credible risk of immediate harm to a pupil;
- failure or absence of filtering or monitoring across a material part of the environment;
- illegal-content protection capable of unauthorised bypass;
- monitoring alerts not being reviewed within the agreed safeguarding process;
- significant gap affecting vulnerable pupils or a whole cohort;
- repeated online-safety incidents indicating systemic weakness;
- material data, cyber or supplier incident with safeguarding implications;
- West Lodge transitional risk above tolerance; and
- action overdue where the continuing risk is high.

The SDEG digital-safeguarding test
Are pupils educated? Are controls appropriate? Are alerts acted upon? Do vulnerable pupils receive what they need? Can leaders demonstrate that the arrangements work?