DIGITAL SERVICES, INFORMATION SECURITY & CYBER RESILIENCE POLICY

Policy Owner:	Chief Operating Officer (COO)
ISSR Reference:	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 Group-wide governance, minimum controls, resilience expectations, assurance and transition arrangements for digital services and cyber resilience.

1. Aims

This Policy creates the overarching Group framework for digital services, information security and cyber resilience. It centralises infrastructure, security, compliance, service-management and legislative requirements for all Group schools and professional services, while preserving school-level ownership of educational delivery, pupil behaviour, age-appropriate digital curriculum and local operating routines.

The centralisation principle
For schools operating on the Group digital environment, infrastructure, platforms, identity, information security, cyber controls, technical compliance, backup, service continuity and technical assurance are centrally governed and managed. Schools remain accountable for safe local use, educational delivery, safeguarding response and compliance by their staff and pupils.

1.1 Purpose

SDEG relies on digital services to educate pupils, safeguard the community, communicate, manage operations and protect charitable assets. This Policy establishes how the Group will govern, design, secure, operate, recover and assure its digital environment so that technology enables Excellence. Differently. without exposing pupils, people, information or services to unmanaged risk.

1.2 Scope

The Policy applies to all networks, devices, applications, cloud services, communications platforms, data stores, identity services, websites, telephony, audio-visual systems, Internet of Things devices, backups and third-party digital services owned, licensed, managed or used for Group activity. It applies to governors, employees, pupils, volunteers, contractors, agency workers, visitors and suppliers with authorised access.

1.3 Tier 1 relationship

This Policy sets mandatory Group outcomes and minimum standards. It is supported by the other Tier 1 digital policies, including Digital Safeguarding & Online Safety, Digital Communications & Acceptable Use, and AI & Emerging Technologies. Detailed procedures, architecture records, standards, asset registers, service catalogues, incident playbooks and school Digital Curriculum & Delivery Statements sit below the Tier 1 suite.

1.4 Non-contractual status

This Policy does not form part of any employee's contract. Breach may be addressed under the applicable disciplinary, pupil behaviour, contractual or governance process. Nothing in this Policy limits statutory safeguarding, data-protection or incident-reporting duties.

SDEG will maintain digital services that are secure, proportionate, resilient, supportable and aligned with educational and operational purpose. Security will be designed into services, not

added after deployment. Access will follow least privilege. Information will be protected according to sensitivity. Critical services will have tested continuity and recovery arrangements. Incidents and weaknesses will be reported early, contained, investigated and learned from.

The Group will balance security, safeguarding, privacy, accessibility, educational benefit, affordability and usability. Controls should enable excellent education and responsible innovation while preventing avoidable harm and unmanaged dependency.

2. Legislation and Regulatory Framework

This Policy is informed by applicable law, statutory guidance and recognised standards, including:

- UK General Data Protection Regulation and Data Protection Act 2018;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) Regulations 2000;
- Copyright, Designs and Patents Act 1988;
- Education (Independent School Standards) Regulations 2014;
- Keeping Children Safe in Education 2026;
- Early Years Foundation Stage statutory framework;
- Prevent duty guidance;
- Department for Education digital and technology standards for schools and colleges, including the cyber-security core standard;
- Department for Education filtering and monitoring standards;
- UK Safer Internet Centre appropriate filtering and monitoring definitions; and
- National Cyber Security Centre guidance for schools, boards, staff and technical teams.

The Group will maintain a compliance mapping record linking this Policy and its supporting controls to relevant statutory, regulatory, insurance and contractual obligations. The Independent School Standards do not prescribe a standalone digital-services policy, but this Policy supports safeguarding, pupil welfare and effective leadership and management through defined controls and assurance.

3. Roles and responsibilities

3.1 Group Board of Governors

- approve this Policy and hold the Chief Executive Officer to account for implementation;
- ensure digital and cyber risk is considered within the Group risk framework;
- receive assurance on critical services, cyber posture, material incidents, recovery readiness and significant investment;
- ensure appropriate capability, resources and independent assurance; and
- satisfy itself that safeguarding-related filtering and monitoring responsibilities are discharged.

3.2 Group Board of Governors

- scrutinise cyber, information-security, resilience and third-party risk;
- review dashboards, control exceptions, incidents, overdue actions and assurance findings;
- test whether remediation is timely and proportionate; and
- recommend escalation or investment to the Group Board.

3.3 Group Board and Safeguarding Link Governor

- receive assurance on the safeguarding effectiveness of filtering and monitoring;
- review themes, limitations, significant online-safety incidents and annual effectiveness review;
- ensure technical assurance is connected to DSL judgement and pupil needs; and
- avoid assuming operational responsibility for systems or case management.

3.4 Local School Boards

- receive proportionate local assurance on service experience, safeguarding effectiveness and material transition risks;
- support and challenge the Head regarding local implementation and educational impact; and
- escalate recurring or material concerns through the Group governance route.

3.5 Chief Operating Officer

- hold executive accountability for the Group digital environment;
- ensure sufficient leadership, resources, prioritisation and cross-Group co-operation;
- approve material risk acceptance and major recovery or migration decisions;
- ensure significant incidents are reported to the Chair and relevant bodies; and
- sponsor the planned migration of West Lodge to the Group operating model.

3.6 Chief Operating Officer

- own this Policy and the Group digital operating model;
- align digital strategy, investment, service design and transformation with Group priorities;
- chair or commission prioritisation of significant digital change;
- ensure commercial, supplier, data, cyber, resilience and educational considerations are integrated;
- hold the Director of Digital Services to account for control operation and service performance; and
- report assurance, decisions and material risks to the Chief Executive Officer and governance bodies.

3.7 Director of Digital Services

- operate and continuously improve the Group technical control environment;
- maintain architecture, asset, system, supplier and privileged-access records;
- secure networks, devices, identities, cloud services, backups and technical integrations;
- lead technical incident response and recovery;
- maintain patching, vulnerability, configuration, logging and monitoring arrangements;
- provide technical support for filtering and monitoring and evidence for the annual safeguarding review;
- ensure changes are tested, authorised, documented and recoverable; and
- provide accurate service, security and resilience reporting.

3.8 Heads

- ensure staff and pupils comply with Group digital policies;
- own safe and effective local use and educational delivery;
- ensure the DSL and Digital Services receive timely information about needs, incidents and emerging risks;
- authorise local priorities and escalation within the agreed governance model;
- ensure local continuity arrangements can operate during digital disruption; and
- for West Lodge during transition, ensure approved local controls are maintained and evidenced.

3.9 Designated Safeguarding Leads

- lead safeguarding judgement about online risk and monitoring response;
- understand the capabilities and limitations of local filtering and monitoring;
- work with the responsible SLT member and Digital Services on the annual effectiveness review;
- ensure safeguarding alerts and incidents are triaged, recorded and acted upon;
- identify vulnerable cohorts and changing safeguarding needs; and
- escalate control gaps immediately.

3.10 Group Director of Governance & Compliance

- connect material digital risks, incidents and actions to the Risk, Assurance & Compliance Framework;
- include proportionate independent digital assurance within the Annual Audit & Assurance Plan;
- advise on governance evidence, escalation and action tracking; and
- verify closure of material findings where appropriate.

3.11 Data Protection Officer and Information Asset Owners

- advise on lawful processing, privacy risk, DPIAs, breach assessment and data-subject rights;
- maintain accountability records required by data-protection law;
- ensure assets have accountable business owners and appropriate classification; and
- support decisions about retention, sharing, access and disposal.

3.12 All users

- use only authorised systems and access;
- protect credentials, devices and information;
- complete required training;
- report suspected phishing, loss, weakness, breach or unusual activity immediately;
- comply with acceptable-use, safeguarding, data-protection and records requirements; and
- co-operate with containment, investigation and recovery.

4. Digital services, information security and cyber resilience framework

4.1 Core principles

Principle	Application
Educationally enabling	Digital services support learning, safeguarding, inclusion, communication and efficient operations.
Secure by design	Security, privacy, supportability and recovery are considered before approval or deployment.
Centrally governed	Infrastructure, cyber controls, technical standards and platform assurance are Group responsibilities except under an approved transition arrangement.
Safeguarding-led	Filtering, monitoring and incident response connect technical capability with safeguarding judgement.
Least privilege	Users receive only the access required, for only as long as required.
Defence in depth	People, process and technical controls work together; no single control is treated as sufficient.
Recoverable	Critical data and services have protected backups, recovery objectives and tested restoration arrangements.
Evidence-based	Key controls have named owners, records of operation and proportionate independent assurance.
Proportionate	Controls reflect information sensitivity, pupil risk, service criticality, threat and educational impact.
Transparent and accountable	Users understand monitoring, responsibilities, reporting routes and consequences of misuse.

Continuously improving	Incidents, near misses, audits, threat intelligence and user feedback drive improvement.
Future-ready	Architecture and investment consider sustainability, interoperability, accessibility and emerging technology.

4.2 Digital services management system

Stage	Minimum expectation
Plan	Maintain strategy, architecture, standards, risk assessment, priorities, resources, owners and recovery objectives.
Protect	Implement identity, device, network, cloud, data, supplier and user controls.
Detect	Collect relevant logs, monitor alerts, test controls, gather user reports and review threat information.
Respond	Triage, contain, preserve evidence, communicate, fulfil reporting duties and maintain safeguarding response.
Recover	Restore priority services and data safely, validate integrity, communicate status and manage return to normal.
Learn	Review root causes, control performance, decisions and impacts; assign and verify improvements.

4.3 Minimum digital and cyber controls

7.1 Asset, architecture and service ownership

- maintain current registers of hardware, software, cloud services, information assets, IoT devices, suppliers and accountable owners;
- identify service criticality, data sensitivity, dependencies, support arrangements and recovery requirements;
- document significant architecture and data flows; and
- retire unsupported, duplicate or unjustified technology through controlled change.

7.2 Identity and access management

- unique user identities and approved authentication;
- multi-factor authentication wherever required by the Group standard, particularly for privileged and remote access;
- least privilege, role-based access and segregation of duties;
- controlled joiner, mover and leaver processes with prompt removal of access;
- separate, restricted and monitored privileged accounts;

- termly review of privileged and high-risk access, and periodic review of other access; and
- prohibition of shared credentials except for a documented, risk-assessed technical necessity.

7.3 Secure configuration, patching and vulnerability management

- standard secure configurations for managed devices and services;
- supported operating systems, applications and firmware;
- timely security updates and remediation prioritised by risk;
- anti-malware or equivalent endpoint protection where appropriate;
- firewalls and network controls protecting all connected technology, including IoT;
- regular vulnerability assessment and proportionate penetration or security testing; and
- documented exceptions with owner, risk, controls and expiry.

7.4 Network and cloud security

- segmentation appropriate to users, devices, services and safeguarding risk;
- secure wireless configuration and controlled guest access;
- central administration and logging of critical network services;
- secure remote access;
- approved cloud services with appropriate contracts, security, privacy, exit and recovery arrangements; and
- protection against malicious domains, email threats and unauthorised data transfer.

7.5 Data and information security

- classification and handling according to sensitivity;
- need-to-know access and approved storage locations;
- encryption in transit and at rest where required;
- secure sharing, transfer, retention and disposal;
- clear-desk and physical-security controls for paper and removable media;
- prohibition on using unauthorised services for Group information; and
- DPIAs and specialist review where processing creates high privacy risk.

7.6 Backups and recovery

- documented backup scope, frequency, retention, protection and ownership;
- backups protected from alteration or compromise by the production environment;
- regular monitoring of backup completion;
- restoration tests proportionate to criticality, with results and actions recorded;
- recovery priorities, dependencies and decision-makers aligned with business continuity plans; and
- offline working and manual fallback where necessary for critical safeguarding or operational activity.

7.7 Logging, detection and monitoring

- logging proportionate to security, safeguarding, legal and operational needs;
- time synchronisation and retention sufficient to support investigation;
- monitoring of critical security events, privileged activity and service health;
- alert triage with named responsibility and escalation criteria; and
- lawful, transparent and proportionate monitoring consistent with privacy notices and the Digital Communications & Acceptable Use Policy.

7.8 Technical change and procurement

- business ownership and defined purpose before procurement or deployment;
- security, privacy, safeguarding, accessibility, interoperability, support, sustainability and exit assessment;
- technical approval by Digital Services;
- DPIA and contractual review where required;
- testing, change approval, implementation and rollback arrangements; and
- updates to asset, architecture, support and recovery records.

7.9 Supplier and third-party risk

- due diligence proportionate to service criticality and data handled;
- clear security, privacy, incident, availability, backup, subcontracting and exit obligations;
- named Group owner and supplier contact;
- review of assurance evidence and material changes;
- prompt notification and co-operation during incidents; and
- contingency arrangements for critical supplier failure.

4.4 Filtering and monitoring interface

The detailed safeguarding framework sits in the Group Digital Safeguarding & Online Safety Policy. Under this Policy, Digital Services must provide technically appropriate filtering and monitoring controls, document coverage and limitations, maintain technical records, test operation and support safeguarding review and response.

At least once in every academic year, the nominated senior leadership member responsible for filtering and monitoring will lead and document a review of effectiveness, supported by the relevant DSL and Digital Services. The review will consider current provision, gaps, pupil and staff needs, devices, apps, remote use, user attribution, alert handling, dynamic and AI-generated content, and the educational impact of over-blocking.

Illegal-content protections and other mandatory controls must not be capable of casual bypass. Any authorised bypass or exception must be necessary, time-limited, recorded, technically controlled and capable of review.

4.5 Cyber incident management and resilience

9.1 Report immediately

Actual or suspected cyber incidents, data breaches, credential compromise, malware, ransomware, loss of devices, unauthorised access, significant service outage or safeguarding-related control failure must be reported immediately through the published route. Users must not investigate or remediate independently unless instructed.

9.2 Severity and command

The Director of Digital Services leads technical response. The Chief Operating Officer provides executive co-ordination within delegated authority. The Chief Operating Officer provides executive command for a major digital incident, escalating to the Chief Executive Officer where the incident has material Group-wide, strategic or reputational implications. The DSL leads safeguarding response; the DPO leads data-protection assessment; Communications, People, Estates, Finance and Governance & Compliance support according to impact.

9.3 Response requirements

- protect life and safeguard pupils first;
- contain harm and preserve evidence;
- establish facts, affected services, data, users and dependencies;
- activate business-continuity and recovery arrangements;
- maintain a decision and action log;
- communicate accurately on a need-to-know basis;
- consider notification to insurers, law enforcement, regulators, affected individuals and other bodies;
- restore from trusted sources and validate integrity before return to service; and
- complete a lessons-learned review and track actions to verified closure.

9.4 Exercises and testing

The Group will test cyber response and recovery arrangements periodically and after material change. Exercises must include leadership decisions, communications, safeguarding continuity, technical recovery and critical manual workarounds. Material findings are reported through the assurance framework.

4.6 Service continuity and disaster recovery

Critical area	Continuity expectation
Safeguarding and welfare	Access to essential safeguarding information, contact routes and incident reporting.
Identity and communications	Authentication, core email/collaboration and emergency communications.
Management information	Pupil, attendance, contact and operational records required to run schools safely.

Teaching and learning	Priority learning platforms, devices, printing and classroom connectivity.
Finance and payroll	Critical payment, payroll and financial-control activity.
Premises and security	Access control, telephony, CCTV or other digitally dependent safety systems where applicable.
Backups and recovery	Protected recovery data, documented sequence and validated restoration.

Each critical service must have an owner, impact assessment, recovery objective, dependencies, fallback, supplier contact and tested recovery method. Recovery priorities are approved through the Group continuity framework and reviewed after significant system change.

4.7 West Lodge transitional arrangements

Transitional status
West Lodge School joins SDEG on 1 September 2026. Because of infrastructure and system constraints, full technical migration to the Group digital operating model is planned for September 2027. This is a controlled transition, not an exemption from safeguarding, legal, risk or reporting duties.

11.1 Requirements applying from 1 September 2026

- Group governance, risk, assurance and incident-escalation requirements;
- safeguarding and online-safety duties, including effective filtering and monitoring review;
- data-protection, confidentiality and breach-reporting requirements;
- cyber-risk assessment and recording of material control gaps;
- mandatory staff awareness and training requirements;
- supplier and change notification to the Group digital leadership; and
- co-operation with migration planning, audit and evidence requests.

11.2 Approved transitional variation

West Lodge may continue to operate approved local infrastructure, systems, device management, identity, filtering, monitoring and support arrangements until migration. The Chief Operating Officer and Director of Digital Services will maintain a West Lodge Digital Transition Plan and Exception Register, approved by the Chief Executive Officer.

Each exception must identify the Group requirement not yet met, reason, current control, residual risk, accountable owner, evidence, migration dependency, target date and escalation threshold. Transitional operation must not be described as full Group technical compliance.

11.3 Migration assurance

- baseline asset, system, supplier, contract, data, network and cyber-risk assessment;
- safeguarding review of filtering and monitoring;
- target architecture and migration sequence;
- data migration, retention and disposal controls;
- identity and access transition;
- backup, rollback, continuity and incident arrangements;
- staff and pupil communication and training;
- readiness review before cutover; and
- post-migration validation and closure of exceptions.

11.4 Governance

Progress and material risks will be reported at least termly to the Chief Executive Officer and relevant governance body during the transition year. Any material delay, safeguarding weakness or risk above tolerance must be escalated through the Group Risk, Assurance & Compliance Framework.

4.8 Training, awareness and culture

All users will receive role-appropriate information and training. Staff complete cyber-security awareness at induction and annually thereafter, with updates when threats or controls change. Privileged users, leaders, DSLs, service owners and incident-team members receive additional training appropriate to their responsibilities.

Awareness will cover phishing and social engineering, credential and device protection, secure information handling, incident reporting, safeguarding interfaces, approved systems, remote working and relevant emerging threats. Training completion and effectiveness will be monitored, with targeted intervention where risk or behaviour indicates need.

4.9 Assurance, metrics and reporting

Assurance area	Minimum evidence
Governance	Material risks, decisions, exceptions, investment and overdue actions.
Assets and support	Coverage and accuracy of asset, system, ownership and support records.
Identity	Joiner/mover/leaver timeliness, privileged-access review and MFA coverage.
Vulnerability	Supported technology, security updates, vulnerabilities and approved exceptions.
Protection	Endpoint, firewall, email, backup and recovery-control operation.
Detection and response	Alerts, incidents, containment, reporting and lessons learned.
Resilience	Backup success, restoration tests, exercises and critical-service recovery readiness.

People	Training completion, phishing or awareness indicators and targeted support.
Suppliers	Critical supplier assurance, incidents, concentration and exit risk.
West Lodge transition	Milestones, exceptions, residual risks and migration readiness until closure.

The Chief Operating Officer will provide termly management assurance to the Chief Executive Officer and proportionate reporting to the Group Board. Safeguarding-related assurance will also be reported through the Group Board. The Group Board receives an annual effectiveness review and prompt reporting of material incidents or risks.

Independent or second-line assurance will be included in the Annual Audit & Assurance Plan according to risk. Findings must have an owner, due date and evidence of verified closure.

4.10 Records and controlled supporting documents

Controlled record	Purpose
Digital asset and systems registers	Hardware, software, cloud, IoT, owners, support, data and criticality.
Architecture and data-flow records	Key systems, integrations, dependencies and transfers.
Access and privileged-account records	Approval, role, review, change and removal.
Cyber risk and exception register	Risk, control gap, owner, action, expiry and acceptance.
Supplier register	Service, contract, data, owner, assurance, incident and exit information.
Backup and recovery records	Scope, results, tests, failures and remediation.
Incident and decision logs	Timeline, evidence, impact, notifications, recovery and learning.
Filtering and monitoring technical record	Coverage, configuration principles, tests, limitations and annual review evidence.
West Lodge Transition Plan	Milestones, dependencies, risks, exceptions, readiness and closure.
Service continuity and recovery plans	Priority, objective, dependencies, fallback, contacts and recovery method.

Product names and detailed configurations must be kept in controlled operational records rather than this Tier 1 Policy. Records will be retained, accessed and disposed of in accordance with the Data Retention Policy and applicable legal or evidential requirements.

4.11 Implementation and transition actions

Action	Owner	Timing	Evidence
Approve digital Tier 1 architecture	Chief Operating Officer	Policy adoption	Confirmed policy map, ownership and

			superseded documents.
Create Group technical standards and registers	Director of Digital Services	Following adoption	Controlled standards, asset/system register, cyber exception register and service catalogue.
West Lodge baseline and transition plan	Chief Operating Officer / Director of Digital Services	At the start of the transition year	Approved baseline, target architecture, milestones, owners and risk treatment.
Review filtering and monitoring arrangements	Responsible SLT lead, DSL and Digital Services	Once each academic year	Documented effectiveness review and tracked actions.
Align business continuity and recovery	CEO and service owners	During 2026/27 assurance cycle	Critical services, recovery objectives, tested plans and actions.
Cross-document rationalisation	Policy owners	Following approval of the Tier 1 digital suite	Infrastructure and compliance content removed from school policies; educational delivery retained in local statements.

5. Monitoring

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

- legislative change;
- regulatory change;
- a material cyber or data incident;
- a major service or organisational change;
- a significant threat development;
- evidence that controls are ineffective.

Monitoring and assurance activity will include risk reporting, asset and access reviews, vulnerability management, backup and recovery testing, incident analysis, supplier assurance, training compliance and independent assurance.

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

6. Links with other policies

- Risk, Assurance & Compliance Policy;
- Digital Safeguarding & Online Safety Policy;
- Digital Communications & Acceptable Use Policy;
- AI & Emerging Technologies Policy;
- Data Protection Policy and privacy notices;
- Data Breach and Incident Response Procedure;
- Data Retention Policy;
- Business Continuity and Critical Incident arrangements;
- Safeguarding and Child Protection Policies;
- Staff Code of Conduct;
- school Digital Curriculum & Delivery Statements;
- supplier contracts, service management procedures and technical standards; and
- West Lodge Digital Transition Plan and Exception Register.

Appendix 1: Digital assurance and escalation framework

Layer	Frequency	Owner	Evidence
Operational control	Continuous / scheduled	Digital Services and control owners	Service records, alerts, maintenance, access, backup and incident evidence.
Management review	Monthly / termly as appropriate	Director of Digital Services and Chief Operating Officer	Dashboard, risks, exceptions, projects, suppliers and recovery readiness.
Safeguarding assurance	At least annually and termly reporting as relevant	SLT filtering/monitoring lead, DSL and Digital Services	Effectiveness review, incidents, limitations and actions.
Second-line assurance	Risk-led	Governance & Compliance / DPO / specialist reviewer	Control testing, compliance mapping and action verification.
Governance scrutiny	Termly and annual	ARC, Group Board, Group Board	Material risks, trends, incidents, investment and annual effectiveness review.
External assurance	Risk-led and planned	Independent specialist / auditor	Cyber, resilience, compliance or technical testing.

Appendix 2: Material escalation triggers

- credible risk of harm to a pupil or failure of a safeguarding control;
- unauthorised access to, loss of or significant compromise of personal or confidential information;
- ransomware, destructive malware or compromise of privileged credentials;
- critical service outage beyond the approved tolerance or with significant educational impact;
- failure or absence of recoverable backups for a critical service;
- evidence of active exploitation, persistent attacker access or significant supply-chain compromise;
- material legal, regulatory, contractual or insurance notification requirement;
- repeated control failure or overdue high-risk remediation;
- West Lodge transition risk above tolerance or material migration delay; and
- incident likely to cause significant financial, operational or reputational impact.

Any person identifying a trigger must report it immediately. The relevant functional lead will protect pupils and services, establish command and escalate to the Chief Executive Officer, Chair, regulators, insurers or external agencies as required by the circumstances and applicable procedures.

The SDEG digital-resilience test
Do we know what we depend on? Is it appropriately protected? Would we detect failure or attack? Can we operate and recover? How do we know?