



Risk and Compliance

Policy Owner: Chief Operating Officer (COO)

ISSR Reference: N/A

Review: Lent 2026

Approved: Governing Body – Lent 2026

Next Review: Lent 2027

Version control information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Operating Officer	Lent 2025	Transfer to new template
Annual review	Chief Operating Officer	Lent / Spring 2026	No changes to policy or procedure Minor edits only

Contents

1. Aims and introduction	2
2. Legislation and definitions	3
3. Roles and responsibilities	4
4. Risk identification and mitigation	5
5. Training and awareness.....	10
6. Reporting risk and escalation	10
7. Monitoring.....	11
8. Links with other policies	11
Appendix A: Risk matrix	12
Appendix B: Key Performance Indicators (KPIs).....	13
Appendix C: Logs.....	14

1. Aims and introduction

This policy is applicable to all staff and outlines the approach taken to identifying, assessing, mitigating and monitoring risks, and ensuring compliance with legal and regulatory obligations, as well as representing our ethical obligations and organisational values. The policy supports the safeguarding of staff, pupils, visitors and assets, as well as the sustainability of St Dunstan’s Education Group’s operations.

St Dunstan’s Education Group (the Group) aims to:

- Establish a consistent approach to ensuring compliance with all laws, regulations and standards across all schools in the Group
- Establish a consistent approach to identifying and managing risk across all schools in the Group
- To protect all staff, pupils, visitors, premises and assets by identifying and managing risks
- To embed a culture of accountability and continuous improvement
- To ensure that all risk-related concerns are reported promptly via clear reporting mechanisms and that all staff understand that they can report risk and compliance concerns without fear of retaliation.

2. Legislation and definitions

2.1 Legislation

This policy is informed by the following legislation and regulatory bodies:

- Charities Act 2011
- Charity Statement of Recommended Practice (SORP)
- The Education Act 2002
- Employees Rights Act 1996
- The Employment Relations Act 1999
- Equality Act 2010
- Financial Reporting Standards (FRS) 102
- The Health and Safety at Work etc. Act 1974
- The General Data Protection Regulation
- Independent Schools Inspectorate Standards (ISI)
- UK Visa and Immigration (UKVI)

2.2 Definitions

Compliance	Adherence to laws, regulations and policies.
Control measures	Actions or processes put in place to manage or reduce risk.
Independent Schools Inspectorate (ISI)	The organisation responsible for inspecting independent schools for compliance and quality assurance.
Risk	The possibility of an event / outcome occurring that may negatively impact the Group's objectives.
Risk management	A systematic process of identifying, assessing, mitigating and monitoring risks to ensure the Group's objectives are met.
Risk register	A document listing all identified risks, the risk rating and agreed controls / mitigations.
Residual risk	The remaining levels of risk after mitigation measures have been applied.
UKVI	UK Visas and Immigration, the government body responsible for immigration and visa compliance.
Whistleblowing	The act of reporting concerns about risks, misconduct, breaches of compliance, or unethical practices within the organization, without fear of retaliation.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The governing body has ultimate responsibility for the management of risk and compliance but will delegate day-to-day responsibility to the Chief Executive Officer. The governing body has a responsibility to:

- Review annually this Risk and Compliance Policy and all associated policies and procedures
- Ensure that risk management and compliance efforts are fit for purpose
- Determine the Group's risk appetite in a range of areas
- Review the Group's risk register termly
- Ensure a robust and fair Whistleblowing Policy is in place
- Appoint one governor to have particular responsibility for health and safety and one governor to have particular responsibility for safeguarding that will regularly 'deep dive' into the organisation and test policies and practices.

3.2 Chief Executive Officer

The Chief Executive Officer (CEO) has a responsibility to:

- Determine the Group's risk management strategy by developing and maintaining the Group's risk management framework
- Monitor the risk registers of the individual schools and combine these into a Group-level risk register
- Oversee professional services departments to ensure proper risk mitigation measures are in place
- Ensure adequate resource and support is in place to effectively manage risk and compliance across the Group
- Promote awareness of the Whistleblowing Policy and ensure concerns are escalated appropriately.

3.3 The Heads of the schools

The Heads of the schools are responsible for:

- Overseeing the implementation of risk management and compliance frameworks for their respective schools
- Monitoring the risk register of their school and contributing to the Group-level risk register
- Maintaining the serious incident log for their school
- Leading on critical incidents in their school

- Ensuring that adequate resource and support is in place to effectively manage risk and compliance in their school
- Providing termly updates on risk and compliance in their school to the governing body
- Promoting awareness of the Whistleblowing Policy and ensuring concerns are escalated appropriately.

3.4 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Developing and overseeing the implementation of risk management and compliance frameworks for health and safety, data protection and people management
- Providing termly updates to the governing body on health and safety, data protection and people management
- Ensuring that there is a suitable and sufficient critical incident plan in place for each of the schools and acting as the operational lead for critical incidents
- Maintaining the Group-level serious incident log.

3.5 Chief Financial Officer

The Chief Finance Officer (CFO) is responsible for:

- Overseeing the implementation of risk management and compliance frameworks for finance
- Overseeing all financial controls, ensuring adherence to legal and regulatory requirements including the Financial Reporting Standards and Charity Statement of Recommended Practice
- Providing termly updates to the governing body on finance-related risks.

3.6 School Designated Safeguarding Leads

Each school's Designated Safeguarding Lead (DSL) is responsible for:

- Overseeing the implementation of risk management and compliance frameworks for safeguarding in their school
- Ensuring their school's Child Protection and Safeguarding Policy and procedures are effectively implemented
- Monitoring and reporting on safeguarding risks and concerns to the Head of their school.

4. Risk identification and mitigation

The Group seeks to mitigate both immediate and perennial risk to tolerable levels. The primary mechanism for achieving this is through regular reviews of risk at senior leadership, executive and

governance level.

The primary mechanisms for recording, evaluating and mitigating against risk are the school-level and Group risk registers and the serious incident logs.

4.1 Senior leadership team risk mitigation

The senior leadership teams (SLT) of each school are responsible for:

- Weekly review of ‘emerging persistent risks and modifications to the risk register’ as a standing item on the SLT agenda
- Weekly review of ‘updates on current risks and modifications to serious incident log’ as a standing item on the SLT agenda
- Termly review of the serious incident log to look for trends and appropriate mitigations and actions
- Termly detailed review of the risk register and consideration given to Group-level risks
- Termly reviews of other logs that present risk to the school, including but not limited to bullying, behaviour, GDPR breaches and staff absence
- Termly review of the individual schools’ and Group’s Key Performance Indicators (KPIs) as detailed in Appendix B.

4.2 Executive risk mitigation

The Executive Team (DET) routinely review risks as follows:

- Twice termly review of ‘emerging persistent risks and modifications to the risk register’ as a standing item on the DET agenda
- Twice termly review of ‘updates on current risks and modifications to serious incident log’ as a standing item on DET agenda
- Termly review of the serious incident log to look for trends and appropriate mitigations and actions
- Termly detailed review of the schools’ and Group’s risk registers
- Termly reviews of other logs that present risk to the Group including, but not limited to, bullying, behaviour, debtors, GDPR breaches and staff absence
- Termly review of KPIs as detailed in Appendix B.

4.3 St Dunstan’s Education Group risk mitigation

The governors of St Dunstan’s Education Group hold overall responsibility for the identification and mitigation of risk and ensuring compliance. The governing body meet three times a year to review and offer challenge to DET on the following reports:

- School and Group-level risk registers
- School and Group-level serious incident logs
- Other logs as required, including bullying, individual pupil needs, safeguarding, behaviour, GDPR breaches
- Reports from external auditors (e.g. finance audit, health and safety)
- Reports from the school's Inspection and Compliance Committee.

4.4 External audits and reviews

The Group recognises that to achieve full risk mitigation, appropriate and robust processes of external auditing are imperative. A full list of annual audits is summarised below:

	Purpose	Frequency
Audit: Finances Lead: CFO External provider: HaysMac	Annual financial audit, confirming compliance of financial statements for the Group and SDEG Enterprises Ltd with relevant charity law and UK accounting standards	Annual SDEG audit, Autumn / Spring Includes onsite inspection of files and records
Audit: Teachers' Pension Scheme (TPS) Lead: CFO External provider: RSM	Factual report on the end of year certificate as required by TPS	SDEG audited annually in September
Audit: Safer recruitment Lead: COO External Provider: VWV	Single Central Record inspection to full ISI compliance. Detailed report and action plan provided. Contract also includes all year-round advice and support.	SDEG annual inspection in Michaelmas and all year-round support
Audit: Employment law Lead: COO External provider: HCR	Employment Law advice on all HR Policies and specific employee matters. Including advice and documentation for capability, absence, disciplinary, occupational health, grievance, restructure, redundancy, tribunals.	All year-round telephone and email support
Audit: Health and safety Lead: COO External provider: XSELV and Judicium	Annual site and policy inspection to ensure compliance with health and safety legislation. Covers areas such as site safety, COSHH, fire risk assessment, health and safety training etc. Detailed	Annual inspection at each school and all year-round email and face to face support

	report and action plan provided.	
Audit: Data protection Lead: COO External provider: Judicium	Annual documentation inspection, covering all GDPR policy and procedures. Evidencing good practice regarding breach responses, reporting to ICO, visibility of privacy notices and DPO legal requirements etc.	Annual inspection at each school and all year-round support
Audit: UKVI Lead: COO and Head of St Dunstan's Senior School VWV	Review every three years	Every three years for SDEG
Audit: Safeguarding DSL of each school ISI	TBC	TBC
Audit: ISI Lead: Head of relevant school External provider: ISI	To provide an external 'mock inspection' experience to relevant stakeholders, in particular where there are newly appointed leaders who would benefit from this additional support	As decided by relevant Head of the school

4.5 External advice and support provided on an ad-hoc basis

Area	Purpose	Frequency
Various legal companies DET and Clerk to Governors	Specific one-off advice for various matters including education provision, contracts, finances, VAT etc. usually sought through Rickerbys, RSM or VWV, paid on an hourly basis.	Ad hoc, as and when required

4.6 Risk Registers

Group and school-level risk registers will be used to identify, assess, and manage potential risks that could affect areas such as safeguarding, health and safety, operations, educational outcomes, financial stability and reputation. To compile and update each risk register, each senior leadership

team will adhere to the same risk register format and specifically:

1.	Identify risks	<p>Gather input from key stakeholders (governors, staff, pupils, parents, external experts) and from reviews of KPIs, audit reports etc.</p> <p>Categorises risks into categories such as:</p> <p>Financial e.g. budget constraints, withdrawals, mismanagement. Operational e.g. cybersecurity, infrastructure issues, staffing shortages Legal and compliance e.g. changes in employment law, legal disputes Reputational e.g. complaints, negative publicity Strategic e.g. changes in education policy, loss of leadership, competition from other schools Environmental e.g. weather-related challenges, or sustainability concerns</p>
2.	Identify the strategic area affected	<p>Referring to the Group-strategy, identify the strategic area the risk primarily affects e.g. concerns regarding an increase in debtors would be linked to the strategic area ‘Our business.’ The Group’s strategic areas are:</p> <ol style="list-style-type: none"> 1. Our Education 2. Our pupils – academic and other achievements 3. Our pupils – personal development 4. Our staff 5. Our alumni 6. Our parents and carers 7. Our wider community 8. Our environment 9. Our business
2.	Assess the risks	<p>Estimate the probability of each risk occurring using the scoring matrix 0-5, as detailed in Appendix A.</p> <p>Likelihood estimate the probability of each risk occurring (very low, low, medium, high, very high). Impact evaluate the potential consequences if the risk occurs (very low, low, medium, high, very high). Risk rating combine likelihood and impact to assign a risk rating (e.g. low, medium, high, very high) Prioritise rank risks based on the risk rating so that higher priority risks are addressed first.</p>
3.	Agree mitigation strategies	<p>Identify control measures for each risk, identifying existing controls and any further preventive measures</p> <p>Develop action plans for higher-priority and emerging risks, with specific steps to reduce or mitigate the risk, this includes contingency plans, staff</p>

		training, policy changes etc. Assign a risk owner to ensure commitment to monitoring, managing and mitigating risk
4.	Review and update	The risk register should be reviewed weekly by SLTs, half-termly by DET and termly by the governing body. This is to update existing risks and identify new risks. This regularity of review ensures there is a process for escalating significant or unresolved risks to DET or the governing body promptly. Risk owners' progress with action plans must be monitored by the relevant executive sponsor.
5.	Communicate and report	Updates from the risk register should be shared termly with key stakeholders, for example during Inset sessions. This ensures transparency and collaborative risk management.

5. Training and awareness

All staff receive basic risk assessment training as part of the mandatory Health and Safety Essentials course to ensure they can identify risk and consider appropriate controls. Where appropriate, role holders receive specialist training for areas of risk and compliance specific to their role, for example health and safety, safeguarding and financial management.

Senior leadership teams are expected to engage in risk management training relevant to their specialist areas, maintain business continuity plans and participate in annual critical incident desktop exercises to specifically ensure preparedness for emergencies and high-risk situations.

The Whistleblowing Policy is a mandatory policy that must be read and understood by all new staff and then read annually. The policy is also actively promoted during Michaelmas Inset to ensure all staff understand the procedures for reporting concerns and are reassured that they can act without fear of retaliation.

6. Reporting risk and escalation

All staff are encouraged to share concerns regarding risk and compliance via the normal reporting routes, generally via their line manager.

Health and safety risks must be specifically reported as a 'near-miss' via the relevant school's online accident reporting procedure, as detailed in the relevant Group's Health and Safety Policy.

Staff are expected to immediately report pupil safeguarding risks to their school's DSL in accordance with their school's Child Protection and Safeguarding Policy. Any safeguarding concerns relating to any adult should be reported directly the relevant school head.

Data breaches must be reported immediately via the relevant school's data breach reporting procedure and in accordance with the Group's Data Protection Policy.

The Group also ensures robust whistleblowing procedures are in place, as set out in the Whistleblowing Policy. Whistleblowing procedures are in place for reporting concerns anonymously. Staff are encouraged to use these procedures to escalate concerns promptly, safely and without fear of retaliation.

7. Monitoring

This policy will be reviewed by the COO annually. At every review, the policy will be approved by the Full Governing Body.

8. Links with other policies

This P12 Risk and Compliance policy links to the following policies:

Child Protection and Safeguarding [school]

Complaints [Group]

Risk and Compliance [Group]

Equality and Diversity [Group]

Data Protection and GDPR [Group]

Information Security [Group]

HR [Group]

Finance [Group]

Anti-Fraud Corruption and Bribery [Group]

Whistleblowing [Group]

Appendix A: Risk matrix

Risk matrix					
Likelihood					
Very High	Medium	Medium	High	High	Very High
High	Low	Medium	Medium	High	High
Medium	Low	Medium	Medium	High	High
Low	Low	Low	Medium	Medium	High
Very Low	Low	Low	Low	Low	Medium
	Very Low	Low	Medium	High	Very High
	Impact				

Impact rating guide		
These descriptions will help you decide what impact rating you'll give each risk.		
Impact	Description	Value
Very high	The financial impact in excess of £250k and poses a severe threat to the vision, strategy or reputation of the organisation	5
High	The financial impact will be high (> £130k and < £250k), and/or it has a significant impact on the organisations reputation, strategy and vision organisation	4
Medium	The financial impact will be moderate (>£40k and <£130k), and/or it has no more than a moderate impact on the organisation's reputation, strategy and vision	3
Low	The financial impact is likely to be low and it has a low impact on the organisation's reputation, strategy and vision	2
Very low	Little or no financial or reputational impact	1

Appendix B: Key Performance Indicators (KPIs)

Development	Alumni Engagement Donors
Education	Academic Admissions Behaviour Co-curricular Parent/carer satisfaction Pastoral Pupil satisfaction Retention
Finance	Income Loan covenants Profitability Public benefit Value for money (benchmarking)
Marketing and communications	Awards Event engagement Media interest Parent satisfaction with communications Website traffic
Operations	Cyber resilience audits Data breaches Data protection audits Health and safety audits Help desk response times Subject Access Request compliance
People	Diversity, e.g. pay gap, hiring and promotion rates Recruitment and talent acquisition Pay and benefits benchmarking Staff absence Staff engagement and satisfaction Staff turnover and internal promotion Training completion rates

Appendix C: Logs

Name of Log	Contributors to Log	Purpose of Log	Access to the Log	Review of Log
Student Concerns log (school)	DSLs and deputy DSLs	To record all concerns of a significant nature from parents but below DET level	SLT's	SLT meetings
Stage 1 Concerns log (school)	Head of the relevant school	To record all concerns being handled by DET up to but excluding CEO and Clerk to Governors	SLT's	Annually at DET
Stage 2 and 3 Complaints log (Group)	Clerk to Governors	To record all concerns being handled by the CEO and/or Governing Body – ISI regulations must be followed in recording structure	DET	Annually at FGB3
Serious Misconduct, Bullying, Sexual Harassment and Abuse log (school)	DSLs and deputy DSLs	To record all incidents of bullying and the actions taken – ISI regulations must be followed in the recording structure	DET	Annually at DET
Serious Incident log (school and Group)	Head of the relevant school Chief Operating Officer	To record all serious incidents of whatever nature that present risk to the organisation – to include those	SLT DET	Termly at FGB

		incidents reported to the Charity Commission		
Data Breach log (school)	Head of School Operations Head of Administrative Services School Operations Manager Chief Operating Officer	To record all incidents of data breaches across the schools	Judicium DET	Termly at FGB
Accident Book (school)	Chief Operating Officer Head School of Operations School Operations Manager Head of Health and Safety Director of Estates and Commercial Activities College Nurse	To record all incidents of accidents and near misses across the organisation	DET	Termly at FGB
International Student Register and Change in Circumstances log (school)	Head of Senior School (UKVI Authorising Officer)	To record details of all students for whom we sponsor a visa and any changes to circumstances (including absence)	SLT DET	As required
Health and Safety Logs and Checklists (school)	Head of Health and Safety	A variety of health and safety logs are kept ensuring compliance with	SLT Health and Safety Committees	Termly at FRC

		the Health and Safety Policy	DET	
Safeguarding Log (CPOMS)	DSLs and deputy DSLs	To record all safeguarding concerns	DET and key pastoral staff at varying permissions	Termly at FGB